Cellular Dragnet: Active Cell Site Simulators and the Fourth Amendment

Aimee Thomson[*]

This Paper examines government use of active cell site simulators (ACSSs) and concludes that ACSS operations constitute a Fourth Amendment search. An ACSS—known colloquially as a stingray, triggerfish, or dirtbox—mimics a cell phone tower, forcing nearby cell phones to register with the device and divulge identifying and location information. Law enforcement officials regularly use ACSSs to identify and locate individuals, often with extreme precision, while sweeping up the identifying and location information of hundreds or thousands of third parties in the process. Despite the pervasive use of ACSSs at federal, state, and local levels, law enforcement duplicity concerning ACSS operations has prevented courts from closely examining their constitutionality.

ACSS operations constitute a Fourth Amendment search under both the trespass paradigm and the privacy paradigm. Within the former, an ACSS emits radio signals that trespass on private "effects." Under the Jones *reinvigoration of the trespass paradigm, radio signals "touch" cell phones for the purpose of obtaining information, constituting a "Fourth Amendment trespass." Radio signals also trespass under common law property and tort regimes, and the Paper proposes a new rule, consistent with existing trespass jurisprudence, to target only those radio signals that intentionally and without consent cause an active physical change in the cell phone. Within the latter, ACSS operations constitute a Fourth Amendment search because they violate users' subjective expectations of privacy that society can and should recognize as reasonable, particularly if Fourth Amendment jurisprudence continues to eliminate secrecy as a proxy for privacy. Until courts decisively recognize warrantless ACSS operations as illegal, however, advocates and litigants can implement several interim remedial measures.*

An ACSS is an undeniably valuable law enforcement tool. Subjecting ACSS operations to Fourth Amendment strictures will not hinder their utility but rather ensure that this powerfully invasive technology is not abused.

[*] Candidate for Juris Doctor, May 2015, New York University School of Law. I would like to thank Professor Stephen Schulhofer for his input and guidance and Chris Soghoian for introducing me to cell site simulators. Contact: aimee.thomson@nyu.edu.

I. Introduction

In 1983, the Supreme Court condoned the warrantless tracking of suspected drug manufacturers on public highways, holding that such tracking failed to violate the suspects' reasonable expectation of privacy.[1] Law enforcement had placed a radio transmitter inside a chloroform container that was subsequently sold to one suspect and placed in the car of another.[2] Officers used signals emanating from that transmitter to locate the container—and thus, the suspects—in a remote cabin.[3] The majority dismissed concerns that denying Fourth Amendment protection would result in "twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision."[4] Instead, the Court assured the American public that "if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[5]

Regretfully, neither the Court's optimism concerning government restraint nor the judiciary's place at the vanguard of constitutional interpretation has found fruition. Dragnet, around-the-clock surveillance of the American public has become commonplace.[6] Some has been codified in post-9/11-tinged statutes,[7] some has been extrapolated from tortured interpretations of statutory authority,[8] and some has been born of the opportunistic marriage between sophisticated new technologies and outdated legal standards. This last category represents an especially concerning form of government surveillance, in which dramatic technological advances allow the government to obtain a wide range of sensitive, personal information under the legal blessing of rules never designed to so apply.

One form of increasingly pervasive technology masquerading as a 1980s pen register is the active cell site simulator ("ACSS"), technically known as an International Mobile Subscriber Identity ("IMSI") Catcher and colloquially known as a stingray,[9] a triggerfish,[10] or a dirtbox.[11] First developed in the 1990s,

---

[1] United States v. Knotts, 460 U.S. 276, 285 (1983).
[2] *Id.* at 278.
[3] *Id.* at 278–79.
[4] *Id.* at 283 (internal citation omitted).
[5] *Id.* at 284.
[6] *See, e.g.*, Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 6, 2013), http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers; Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.
[7] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1885(c) (2012). *See* 50 U.S.C. § 1881(a) (2012) ("Procedures for targeting certain persons outside the United States other than United States persons.").
[8] *See* 50 U.S.C. § 1861(a)(1), (b)(2)(A) (2012) (allowing the Foreign Intelligence Surveillance Court to order the protection of "any tangible things" on a showing that "the tangible things sought are *relevant* to an authorized investigation" (emphasis added)); Greenwald, *supra* note 6.
[9] The trademark "StingRay" refers specifically to the active cell site simulator produced by Harris Corporation. *StingRay & AmberJack*, HARRIS CORPORATION, http://files.cloudprivacy.net/Harris_Stingray_product_sheet.pdf (last visited Aug. 12, 2014). Nevertheless, "stingray" has already become the genericized term for active cell site simulators, a use that this Paper adopts.
[10] The trademark "TriggerFish" refers to another ACSS produced by Harris Corporation. *See* Ryan Gallagher, *Meet the Machines That Steal Your Phone's Data*, ARS TECHNICA (Sept. 2013), http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data.

an ACSS mimics cell phone towers.[12] By exploiting cell phones' failure to authenticate networked cell towers, an ACSS tricks cell phones into connecting with it, revealing at minimum the phone's identity and location and at most routing calls and text messages through the stingray to law enforcement officers.[13] ACSSs are now operational by everyone from the National Security Administration ("NSA") in Afghanistan[14] to the Gwinnett County Police in Lawrenceville, Georgia.[15] Despite their operational breadth, however, law enforcement agencies at all levels have failed to disclose their use of ACSSs to the courts, resulting in only a handful of cases where a judge was even given the opportunity to consider whether the devices are constitutional.[16]

ACSS operations threaten fundamental privacy and civil liberties in large part because of the almost ubiquitous ownership of cell phones in modern America. The vast majority of Americans own cell phones, leading the Supreme Court to observe that they "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[17] In addition, unlike other forms of advanced technology such as automobiles or laptop computers, we carry our cell phones with us constantly. As a result, cell phone location has become an effective proxy for the location of the phone's owner. Warrantless ACSS operations, therefore, give the government broad powers to monitor and track all Americans without probable cause or judicial supervision.

This Paper argues that because an ACSS both physically intrudes upon a person's effects and violates a person's reasonable expectation of privacy, government use of an ACSS qualifies as a Fourth Amendment search. As a result, law enforcement officials should not operate an ACSS without probable cause and a warrant or warrant exception.

Part II details how an ACSS functions, with an emphasis on its ability to collect cell phone location information, and outlines at least five ways that law enforcement officials can and do operate ACSSs. Part III briefly summarizes the existing Fourth Amendment framework applicable to electronic and tracking surveillance, concluding with a brief discussion about the inapplicability of the Third Party Doctrine to ACSS operations. Part IV examines the few cases to date that have expressly involved ACSSs and argues that law enforcement duplicity has improperly restricted the ability of courts to examine the constitutional implications of ACSS operations. Part V explains why government use of an ACSS

---

[11] Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, WALL ST. J. (Nov. 13, 2014), http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533 ("The name 'dirtbox' came from the acronym of the company making the device, DRT, for Digital Receiver Technology Inc. . . . .").

[12] Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1, 14 (Fall 2014).

[13] *Id.* at 12.

[14] Jeremy Scahill & Glenn Greenwald, *The NSA's Secret Role in the U.S. Assassination Program*, THE INTERCEPT (Feb. 10, 2014), https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role/ ("In one tactic, the NSA 'geolocates' the SIM card or handset of a suspected terrorist's mobile phone, enabling the CIA and U.S. military to conduct night raids and drone strikes to kill or capture the individual in possession of the device.").

[15] *Harris Stingray Invoice: Gwinnett County Police Department (2010)*, SCRIBD (July 15, 2014), http://www.scribd.com/doc/233951934/Harris-Stingray-Invoice-Gwinnett-County-Police-Department-2010.

[16] *See infra* Part IV.

[17] Riley v. California, 134 S. Ct. 2473, 2484 (2014).

constitutes a Fourth Amendment search under the trespass paradigm, arguing that the radio signals emitted by an ACSS cause an active physical intrusion consistent with both the *Jones* conception of trespass and the policy rationales underlying existing property and tort jurisprudence. Part VI argues that government use of an ACSS also constitutes a Fourth Amendment search under the privacy paradigm by violating subjective expectations of privacy that society can and should find reasonable. Finally, Part VII identifies several interim mechanisms advocates and litigants can use to impose greater legal restrictions on warrantless ACSS operations.

II. Technology and Function of an Active Cell Site Simulator ("ACSS")

Cell phones are omnipresent in modern society. As the Supreme Court recognized in June 2014, modern cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[18] Ninety-one percent of American adults own a cell phone.[19] Almost 98 percent of America's rural population has coverage by at least one mobile broadband provider, a number that rises to 99.9 percent in non-rural areas.[20] Indeed, as of 2011, there are more operational cell phones than people in the United States.[21]

Not only is cell phone ownership pervasive, but Americans' use of and interaction with their phones are substantial. Indeed, the utility of a cell phone comes from the ability to carry it anywhere and everywhere. In addition to calls, most cell phone owners send text messages, check email, and access the internet with their phones, while one in two owners use location-based services and listen to music.[22] As of 2010, 65 percent of adults sleep next to their cell phones, a figure that rises to 90 percent when looking only at adults aged 18–29.[23] In 2012, two-thirds of cell phone owners checked their cell phones for messages or alerts even when the phone wasn't ringing or vibrating, and nearly one-third describe their phones as "something they can't imagine living without."[24]

This strong attachment to and frequent use of cell phones indicates their central role in modern American life. As a result, the location of a cell phone often serves as a valid proxy for the location of the phone's owner. An ACSS take advantage of this inference, using fundamental principles of wireless telecommunications to identify and track anyone with a cell phone. This Part will first explain the basics of wireless communications and how an ACSS tricks phones into supplying sensitive identifying and location information, then discuss the main ways law enforcement officers can (and do) use ACSSs.

---

[18] *Id.*
[19] Maeve Duggan, *Cell Phone Activities 2013*, PEW RESEARCH INTERNET PROJECT (Sept. 19, 2013), http://www.pewinternet.org/2013/09/19/cell-phone-activities-2013/.
[20] FED. COMMC'N COMM'N, 16TH ANNUAL MOBILE WIRELESS COMPETITION REPORT 28 (2013), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-34A1.pdf.
[21] *Id.* at 10.
[22] *Mobile Technology Fact Sheet*, PEW RESEARCH INTERNET PROJECT, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ (last visited Sept. 17, 2014).
[23] *Do You Sleep with Your Cell Phone?*, PEW RESEARCH INTERNET PROJECT (Sept. 13, 2010), http://www.pewresearch.org/daily-number/do-you-sleep-with-your-cell-phone/.
[24] *Id.*

A. Wireless Communications Systems Facilitate Precise, Real-Time Location Tracking

All cellular devices, including both cell phones and data devices such as tablets, operate using radio signals.[25] Telecommunications carriers "maintain networks of radio base stations (also called 'cell sites')" around the country that make connections between the telephone network and nearby cell phones.[26] Cell sites "divide[] the carrier's coverage area into a mosaic of local 'sectors,' each served by an antenna at a local cellular base station."[27] Each cell site typically has three sectors, each covering approximately 120 degrees of the site's coverage area.[28]

Every few seconds, every powered-on cell phone attempts to register itself with the nearest cell site, defined as the site with the strongest radio signal.[29] Phones are built to optimize reception; if the phone detects more than one cell site belonging to its carrier, "it will always choose the one[] with the strongest signal."[30] Being in constant contact with a base station gives the user "signal" and allows the carrier to correctly route incoming calls.[31] As a user moves throughout her day, her phone will automatically register with the new closest cell site, and any ongoing calls will be ""handed off" between base stations without interruption."[32] During registration, cell phones identify themselves to cell sites with pre-programmed codes identifying "the phone, the phone's owner, and the service provider."[33]

Cell site location information ("CSLI") is data identifying the location of the cell site and sector to which a uniquely identified customer's cell phone sends a signal.[34] As technology advances, CSLI "also reflect[s] the direction of the user from the tower."[35] At minimum, law enforcement officers can

---

[25] *Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance: Hearing Before the H. Subcomm. on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 43 (2013) (testimony of Professor Matt Blaze) [hereinafter Blaze Testimony], *available at* http://www.fas.org/irp/congress/2013_hr/ecpa2.pdf. *See infra* Part V.

[26] *Id.* at 50. Base stations are sometimes called "cellular base stations or sometimes towers or sector antennas." *Id.* at 43.

[27] *Id.* at 53.

[28] *Base stations*, VODAFONE, http://www.vodafone.com/content/index/about/sustainability/mpmh/how_mobiles_work/base_stations.html (last visited Aug. 8, 2014).

[29] Blaze Testimony, *supra* note 25, at 50. *See In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005).

[30] Daehyun Strobel, *IMSI Catcher*, SEMINARARBEIT, RUHR-UNIVERSITÄT BOCHUM 17 (July 13, 2007), *available at* http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf.

[31] *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the H. Subcomm. On the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 14 (2010) (testimony of Professor Matt Blaze), *available at* http://judiciary.house.gov/_files/hearings/printers/111th/111-109_57082.PDF.

[32] Blaze Testimony, *supra* note 25, at 50.

[33] In re *Application*, 396 F. Supp. 2d at 750.

[34] *Id.* at 749 (characterizing cell site data as including "the location of cell site/sector (physical address) at call origination (for outbound calling), call termination (for incoming calls), and, if reasonably available, during the progress of a call" and "information regarding the strength, angle, and timing of the caller's signal measured at two or more cell sites, as well as other system information such as a listing of all cell towers in the market area, switching technology, protocols, and network architecture" (citation omitted)).

[35] United States v. Davis, 754 F.3d 1205, 1211 (11th Cir. 2014), *reh'g en banc granted, opinion vacated*, 573 F. App'x 925 (11th Cir. 2014).

triangulate a user's location by reviewing his CSLI across multiple cell sites.[36] The growing demand for wireless technology, however, has increased the number of cell sites around the country (and correspondingly decreased the geographic coverage area assigned to each site).[37] As a result, a single point of CSLI today could narrow a user's location down to "individual floors and rooms within buildings."[38] Advanced technology further "allows cellular network providers to locate not just the sector in which the users' wireless device is located, but its position *within* the sector."[39] Indeed, network operators can now "pinpoint a phone's latitude and longitude at a level of accuracy that can approach that of GPS."[40]

Functionally, CSLI has two forms. Historical CSLI refers to telecommunications records stored by the carrier "that detail the location of a cell phone in the past."[41] Carriers are under no legal obligation to retain historical CSLI for any length of time,[42] but congressional investigations and Freedom of Information Act requests demonstrate that carriers retain their consumers' historical CSLI anywhere from six months to forever.[43] Prospective or real-time CSLI, by contrast, "refers to data used by the government to identify, with varying degrees of accuracy, the location of a phone at the present moment."[44]

B. An ACSS Tricks Phones into Revealing Sensitive Identifying and Real-Time Location Information

Two types of devices allow law enforcement officials to bypass telecommunications carriers and interact directly with cell phones: passive interception devices and active cell site simulators (ACSSs).[45] Passive interception devices, as the name suggests, intercept the cell signal as it transmits from the phone to the cell site without disrupting the signals in transit.[46] Passive interception devices can "detect the electronic serial number . . . assigned to a particular cellular telephone, the telephone number of the

[36] In re *Application*, 396 F. Supp. 2d at 751.
[37] Blaze Testimony, *supra* note 25, at 53–56.
[38] *Id.*
[39] *Id.* at 56.
[40] *Id.*
[41] Deborah F. Buckman, Annotation, *Allowable Use of Federal Pen Register and Trap and Trace Device to Trace Cell Phones and Internet Use*, 15 A.L.R. FED. 2d 537, at § 2 (2010).
[42] The Federal Communications Commission only requires carriers to retain a narrow subset of consumer data for any length of time. 47 C.F.R. § 42.6 (2014) (requiring that telecoms retain only "the name, address, and telephone number of the caller, telephone number called, date, time and length of the call" for 18 months).
[43] *Retention Periods of Major Cellular Service Providers*, CRYPTOME, http://cryptome.org/isp-spy/cellular-spy3.pdf (last visited May 30, 2014) (noting that T-Mobile retains information about the cell tower used by the phone for six months, while AT&T has retained the same information since July 2008). *See Cell Phone Location Tracking Request Response – Cell Phone Company Data Retention Chart*, ACLU, https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart (last visited May 29, 2014); Press Release, For Second Year in a Row, Markey Investigation Reveals More Than One Million Requests by Law Enforcement for Americans Mobile Phone Data (Dec. 9, 2013), *available at* http://www.markey.senate.gov/news/press-releases/for-second-year-in-a-row-markey-investigation-reveals-more-than-one-million-requests-by-law-enforcement-for-americans-mobile-phone-data; Press Release, Markey: Law Enforcement Collecting Information on Millions of Americans from Mobile Phone Carriers (July 9, 2012), *available at* http://www.markey.senate.gov/news/press-releases/markey-law-enforcement-collecting-information-on-millions-of-americans-from-mobile-phone-carriers.
[44] Buckman, *supra* note 41.
[45] Pell & Soghoian, *supra* note 12, at 9–12.
[46] *Id.*

cellular telephone itself, and the telephone numbers called by the cellular telephone."[47] They can also intercept the content of communications.[48] Passive interception devices can only intercept signals *sent* by a cell phone; as a result, they only function when the cell phone user makes a call.

An ACSS, by contrast, impersonates cell site towers, tricking or forcing cell phones into registering with them instead of the carrier's real cell site tower.[49] Once registered, an ACSS can collect all identifying and location information normally transmitted to the telecommunications carrier, even if the phone is not currently engaged in a call.[50] This information includes the phone's mobile identification number ("MIN"),[51] electronic serial number ("ESN"),[52] international mobile subscriber identity ("IMSI"),[53] international mobile equipment identity ("IMEI"),[54] numbers dialed for both calls and texts, and the phone's current (real-time) location.[55]

An ACSS can be placed in a fixed location, mounted on a car or airplane,[56] or carried by hand, and can be used in two different ways.[57] First, the operator can direct the antenna towards a particular area and collect identifying and location information about all phones in the vicinity.[58] Second, the operator can enter identifying information specific to one phone, pinging only that device.[59] Once that device is

[47] *In re* the Application of the US for an Order Authorizing Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197, 199 (C.D. Cal. 1995).
[48] *Id. See* U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL 40 (rev. June 2005).
[49] Pell & Soghoian, *supra* note 12, at 11; *StingRay & AmberJack*, *supra* note 9 ("*Active* interrogation capability emulates base station to collect MINs and ESNs through *forced* registration . . . ." (emphasis added)). *See* Gallagher, *supra* note 10 (detailing a number of phone interception devices produced by Harris Corporation, including the StingRay, the Gossamer, the Amberjack antenna, and the Harpoon amplifier).
[50] *StingRay & AmberJack*, *supra* note 9 ("[A]ctive approach does not require the target phone to be engaged in a call.").
[51] "The MIN (Mobile Identification Number) is a number that uniquely identifies a mobile telephone *subscriber*. . . . In the United States, the MIN is derived from the 10 digital decimal telephone number assigned to the handset." *MIN (Mobile Identification Number)*, TECH-FAQ, http://www.tech-faq.com/min-mobile-identification-number.html (last visited Aug. 11, 2014) (emphasis in original).
[52] "An Electronic Serial Number is a code created to identify mobile *devices*." *ESN (Electronic Serial Number)*, TECH-FAQ, http://www.tech-faq.com/esn-electronic-serial-number.html (last visited Aug. 11, 2014) (emphasis added).
[53] "IMSI (International Mobile Subscriber identity) is the information that is used for identification of a mobile phone end-user on a network and is uniquely associated with a given cell phone The IMSI code is stored as a 64 bit number or field, and is sent by the mobile phone to the cellular network. The code can also be used by the mobile network to obtain additional information about the phone from the HLR (home location register) or from the visitor location register. In order to help minimize the code from being captured by eavesdroppers, the IMSI code is transmitted as little as possible." *IMSI (International Mobile Subscriber Identity)*, TECH-FAQ, http://www.tech-faq.com/imsi.html (last visited Aug. 11, 2014).
[54] The IMEI is a number unique to a mobile device that "easily identifies a mobile phone being used on a GSM (Global System for Mobile Communications) network." *IMEI (International Mobile Equipment Identity)*, TECH-FAQ, http://www.tech-faq.com/imei.html (last visited Aug. 11, 2014).
[55] John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (June 13, 2014), http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/; *Septier IMSI Catcher*, SEPTIER, http://www.septier.com/146.html (last visited Aug. 11, 2014); *StingRay & AmberJack*, *supra* note 9.
[56] Barrett, *supra* note 11.
[57] *Septier IMSI Catcher*, *supra* note 55.
[58] Jennifer Valentino-Devries, *How 'Stingray' Devices Work*, WALL ST. J. (Sept. 21, 2011), http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/.
[59] *Id.*

located, the ACSS will measure the signal and plot its location on a map; by moving the ACSS around, the operator can then triangulate the phone's location.[60] To facilitate data collection, an ACSS forces phones to run at maximum battery power.[61] Combined with amplifying technology, some ACSSs have an effective range of more than a mile.[62]

Once available only to federal government agencies, ACSSs are now used by many state and local police departments.[63] To date, at least 47 agencies in 19 states and the District of Columbia (eight state police departments[64] plus 39 local police departments in 17 states and the District of Columbia[65]) operate ACSSs, in addition to at least twelve federal agencies, including the FBI, the NSA, the Drug Enforcement Agency ("DEA"), Immigration and Customs Enforcement, the Army, the Navy, and the Marine Corp.[66] In some states, local police departments can borrow ACSSs from state surveillance units[67] or operate them at the request of other counties.[68] Stingrays and other ACSSs cost upwards of $400,000, but the federal government covers most state and local purchases with anti-terror grants.[69] ACSSs have been used at least 1,800 times by the Florida Department of Law Enforcement alone, suggesting that law enforcement officers have used ACSSs in tens or even hundreds of thousands of operations across the country.[70]

---

[60] *Id.*

[61] Joel Hruska, *Stingray, the Fake Cell Phone Tower Cops and Carriers Use to Track Your Every Move*, EXTREME TECH (June 17, 2014), http://www.extremetech.com/mobile/184597-stingray-the-fake-cell-phone-tower-cops-and-providers-use-to-track-your-every-move.

[62] Thom Jenson & Michael Bott, *Is Sheriff's Department Using Tracking and Data-Collecting Device Without Search Warrants?*, NEWS 10/KXTV (June 23, 2014), http://www.news10.net/story/news/investigations/2014/06/23/is-sacramento-county-sheriff-dept-using-stingray-to-track-collect-data/11296461/. *See Harpoon*, HARRIS CORPORATION, http://cdn.arstechnica.net/wp-content/uploads/2013/09/harpoon.pdf (last visited Aug. 12, 2014).

[63] Kelly, *supra* note 55.

[64] In Florida, Illinois, Indiana, Minnesota, New York, Pennsylvania, Texas, and Wisconsin. *Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/maps/stingray-tracking-devices-whos-got-them (last visited Jan. 6, 2015).

[65] In Alaska, Arizona, California, the District of Columbia, Florida, Georgia, Idaho, Illinois, Maryland, Michigan, Minnesota, Missouri, New York, North Carolina, Texas, Virginia, Washington, and Wisconsin. *Id.*

[66] *Id.*

[67] Kelly, *supra* note 55; *Police Use Cellphone Spying Device*, MY FOX NY (May 30, 2014), http://www.myfoxny.com/story/25597191/police-use-cellphone-spying-device ("The county used a $283,000 terrorism prevention grant from the U.S. Department of Homeland Security to pay for the device.").

[68] Kate Martin, *Another Cellphone Surveillance Device In Puget Sound?*, NEWS TRIBUNE (Nov. 6, 2014), http://www.thenewstribune.com/2014/11/06/3475190/another-cellphone-surveillance.html ("Since 2009, the Tacoma Police Department has used its device at the request of other law enforcement agencies, including the Pierce County Sheriff's Department, Lakewood, Kitsap County, King County and others.").

[69] Kelly, *supra* note 55.

[70] Brett Clarkson, *Who's Tracking Your Cellphone Now? Could Be the Cops*, SUN SENTINEL (May 17, 2014), http://articles.sun-sentinel.com/2014-05-17/news/fl-cell-site-simulator-surveillance-florida-20140507_1_stingray-cellphone-simulator ("But Florida Department of Law Enforcement spokeswoman Gretl Plessinger said in an email: 'This technology has been utilized approximately 1,800 times by FDLE and Electronic Surveillance Support Teams.' She said each use by the agency was authorized by a judge."). *See also* Nathan Freed Wessler, *Police Hide Use of Cell Phone Tracker From Courts Because Manufacturer Asked*, ACLU (Mar. 3, 2014), https://www.aclu.org/blog/national-security-technology-and-liberty/police-hide-use-cell-phone-tracker-courts-because ("As two judges noted during the oral argument, as of 2010 the Tallahassee Police Department had used stingrays a staggering 200 times without ever disclosing their use to a judge to get a warrant.").

C. Law Enforcement Can Use an ACSS to Identify, Track, Monitor, Impersonate, and Block Cell Phones

The secrecy surrounding law enforcement use of stingrays and other ACSSs limits our ability to know the full range of potential and actual uses.[71] Nevertheless, several cases in which the government explicitly acknowledged its use of an ACSS have revealed two primary applications: identifying the phone numbers of known individuals, and tracking the location of known phones. In addition, product descriptions from major ACSS suppliers indicate the ability to conduct other invasive operations, including identifying and tracking unidentified phones, intercepting communications content, and blocking a phone's network coverage. All actual and prospective uses of ACSSs raise serious Fourth Amendment concerns.

i. Identify the Phone Number of a Known Individual

Law enforcement officials can deploy an ACSS to identify the phone number of an identified individual whose current phone number is unknown. Identifying the phone number allows the government to track the target and to obtain historical CSLI and other consumer data from the telecommunications carrier. In 1995, the government attempted to obtain a court order to operate a passive interception device "to analyze signals emitting from any cellular phone used by any one of five named subjects of a criminal investigation."[72] The magistrate denied the application because it failed to "specifically identify the cellular phones whose signals it [sought] to analyze."[73] In 2012, another magistrate judge also denied a law enforcement request for a court order "to detect radio signals emitted from wireless cellular telephones in the vicinity of the [Subject] that identify the telephones."[74] Law enforcement explicitly stated that they hoped to determine the target's phone number by "determining the identifying registration data at various locations in which the [Subject's] Telephone is reasonably believed to be operating."[75] And a 2013 affidavit by a DEA agent describes using a digital analyzer "on three occasions in three different locations where [the defendant] was observed to determine the IMSI associated with any cellular telephone being carried by [the defendant]."[76] Law enforcement officials identified the defendant's number by determining that a certain phone was "in the same vicinity in the three separate locations where [the defendant] was observed."[77]

Identifying the phone numbers of known individuals necessarily involves collecting identifying information about cell phones belonging to persons that law enforcement officers cannot identify *ex ante*. Regardless of the government's showing of cause towards the intended target, officials use the ACSS to identify *unknown* phones. Only by collecting information about *all phones* in areas where the known

[71] *See infra* Part IV.
[72] *In re* the Application of the US for an Order Authorizing Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197, 199 (C.D. Cal. 1995).
[73] *Id.* at 201–02. *See infra* Part IV.
[74] *In re* the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012) (internal quotation marks omitted). *See infra* Part IV.
[75] *Id.*
[76] Lukens Aff. 8 n.1, US v. Arguijo (N.D. Ill. Feb. 13, 2012 [*sic*]) (context indicates that filing date was actually Feb. 13, 2013 because the affidavit discusses events occurring as late as Dec. 13, 2012), *available at* http://www.justice.gov/usao/iln/pr/chicago/2013/pr0222_01d.pdf.
[77] *Id.*

individuals operate can law enforcement officers possibly cross-reference common numbers and isolate the suspects' phones. Collecting personal information indiscriminately violates the Fourth Amendment's bedrock principle of particularity.[78] Indeed, the magistrate judge in 1995 expressed concern that "telephone numbers and calls made by others than the subjects of the investigation could be inadvertently intercepted" by passive interception devices.[79] Moreover, because law enforcement officers do not know the location of any phone *ex ante*, the phones (and their owner) could be inside the constitutionally protected space of the home.[80]

ii. Track the Location of an Identified Phone

Mobile, government-operated cell site simulators, combined with advanced technology such as Harris Corporation's AmberJack antenna, further enable law enforcement officers to engage in real-time location tracking of identified cell phones.[81] An ACSS can identify the location of individuals to within ten feet.[82] In 2008, after a woman was raped and had her cell phone stolen, the police used a stingray to track her phone to the suspected perpetrator's house.[83] In 2009, the police used a stingray to track a phone purchased by a defendant moments before he allegedly shot someone outside the store.[84] An officer described the stingray as giving them "an arrow, if you will, pointing to the direction and with the strength tell[ing] [us] how close [we] are to that particular electronic."[85] With the stingray, "officers 'could tell [the target phone] was on the . . . south and east side' of a particular apartment building on the 5700 block of West Hampton Avenue."[86] Also in 2009, a FBI special agent described how he used a stingray "to determine, with a reasonable degree of certainty, a fairly narrow geographical location where an individual is located while a cell call is being placed"—a technique he and those he trained had employed at least 800 times.[87] And in November 2014, the Wall Street Journal revealed the government was mounting ACSS on planes to "locat[e] cellphones linked to individuals under investigation by the government."[88]

In addition, an ACSS allows law enforcement officials to find data devices that might not be easily located by wireless carriers.[89] Data-only devices fall outside of the regulations mandating

---

[78] U.S. CONST. amend. IV ("[N]o warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").
[79] *In re* the Application of the US for an Order Authorizing Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197, 201 (C.D. Cal. 1995).
[80] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 31 (2001) ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" (quoting Silverman v. United States, 365 U.S. 505, 511 (1961))).
[81] *Stingray & AmberJack*, *supra* note 9 ("Interfaces with AmberJack antenna to form a complete target tracking and location solution using active direction-finding and ranging techniques.").
[82] Barrett, *supra* note 11 ("If a suspect's cellphone is identified, the technology can pinpoint its location within about 10 feet, down to a specific room in a building.").
[83] Thomas v. State, 127 So. 3d 658, 659–60 (Fla. Dist. Ct. App. 2013). *See infra* Part IV.
[84] State v. Tate, 849 N.W.2d 798, 801–02 (Wis. 2014). *See infra* Part IV.
[85] *Id.* at 803–04.
[86] *Id.* at 804.
[87] United States v. Allums, No. 2:08-CR-30 TS, 2009 WL 806748, at *1–2 (D. Utah Mar. 24, 2009).
[88] Barrett, *supra* note 11.
[89] Pell and Soghoian, *supra* note 12, at 17–18.

telecommunications carriers to accurately locate cell phones.[90] As a result, "[w]hen the government wishes to locate data-only devices that cannot be precisely located by the wireless carrier, it is likely to turn to active cellular surveillance."[91] In *Rigmaiden*, the IRS traced a number of fraudulent tax returns to an IP address associated with a particular Verizon Wireless broadband air card.[92] Law enforcement used a mobile stingray to measure the aircard's signal at different locations, allowing them "to track the aircard's location to unit 1122 of the Domicilio apartment complex in Santa Clara."[93]

Just like ACSS operations seeking to identify unknown phone numbers, tracking operations can involve the collection of identifying and location information from *all* phones in the vicinity of the device, including from "innocent, non-target" cell phones.[94] Location tracking likewise risks allowing law enforcement officers to gain information from inside the home without a warrant (namely, whether a certain phone, and its owner, are present).

iii. Identify and Track Unidentified Phones Belonging to Unidentified Persons

All publically available information about government use of ACSSs to date has involved some known quantity: either a telephone number/mobile identification number or the identity of the targeted individual. ACSS capacity, however, would easily allow the government to monitor and track unknown phones. Indeed, one ACSS supplier advertises the device's ability to "extract[] identities from [cell phones] in its area of coverage (when these identities are previously unknown)."[95] For example, law enforcement officers might know only that a certain criminal gang frequents several locations in a populated city; to further their investigation, officers might use a stingray to monitor and track what phones frequent all of the locations, collecting the identity and location data from many innocent third-parties in the process. More sinisterly, law enforcement officers might want to monitor large public gatherings in *anticipation* of potential criminal behavior.[96] The ability to conduct this kind of broad surveillance lends itself easily to abuse, and is reminiscent of the general warrants that the Fourth Amendment was created to prevent.[97]

---

[90] *Id.* ("Federal E-911 regulations require that carriers be able accurately to determine the location of cellular phones. As this technical obligation was mandated in the context of E-911, it only applies to devices capable of making a telephone call to 911.").

[91] *Id.* at 18.

[92] United States v. Rigmaiden, No. CR 08–814–PHX–DGC, 2013 WL 1932800, at *1 (D. Ariz. May 8, 2013). "Air cards are devices that plug into a computer and use the wireless cellular networks of phone providers to connect the computer to the internet." Kim Zetter, *Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight*, WIRED (Apr. 9, 2013), http://www.wired.com/2013/04/verizon-rigmaiden-aircard/all/.

[93] *Rigmaiden*, 2013 WL 1932800, at *2.

[94] Aff. of Supervisory Special Agent Bradley S. Morrison, U.S. v. Rigmaiden, No. 2:08-cr-00814-DGC, at *3 (D. Ariz. Oct. 27, 2011) ("During a location operation, the electronic serial numbers (ESNs) (or their equivalent) from all wireless devices in the immediate area of the FBI device that subscribe to a particular provider may be incidentally recorded, including those of innocent, non-target devices."). *See also* Barrett, *supra* note 11 ("The device being used by the U.S. Marshals Service identifies itself as having the closest, strongest signal, even though it doesn't, and forces all the phones that can detect its signal to send in their unique registration information. . . . [T]he device [then] determines which phones belong to suspects and 'lets go' of the non-suspect phones.").

[95] *Septier IMSI Catcher*, *supra* note 55.

[96] Gallagher, *supra* note 10 ("In one case, procurement records (PDF) show cops in Miami obtained a Stingray to monitor phones at a free trade conference held in Miami in 2003.")

[97] *See* Payton v. New York, 445 U.S. 573, 583 (1980) ("It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing

iv. Intercept Incoming and Outgoing Phone and Text Message Content

Although no evidence to date suggests that law enforcement officers are using ACSSs to intercept the content of phone and text message conversations,[98] the capacity to do so undeniably exists.[99] ABILITY's second-generation ACSS, the In-Between Interception System ("IBIS") II, for example, advertises its ability to conduct "Real Time Interception for voice and SMS, Incoming and Outgoing."[100] Intercepting the content of communications triggers a different constitutional question that exceeds the scope of this Paper. As a result, this Paper presumes—in line with current evidence—that law enforcement officers do not use ACSSs to intercept content. Nevertheless, the government's ability to potentially operate a roving wiretap machine should underscore the need for ACSS operations to receive greater judicial scrutiny.

v. Impersonate, Monitor, and Block Cell Phone Calls

Some ACSSs also have abilities beyond identifying and tracking cell phones. ABILITY's original IBIS can conduct man-in-the-middle attacks by intercepting phone signals and impersonating the phone to the network, which allows the device to intercept "incoming and outgoing calls, SMS messages, DTMF tones and all call related information transmitted over the air."[101] The IBIS II can "control the level of service to the target mobiles, selectively Jam specific mobiles, perform silent calls, call or SMS on behalf of target mobile, change SMS messages 'on the fly', detect change of SIM card or change of handset, and support Direction Finding system and many additional operational features."[102]

As with the interception of content, law enforcement officers do not appear to have openly used ACSSs for these purposes. Nevertheless, the mere fact that these devices have the *capacity* to impersonate, monitor, intercept, and block cell phone calls heightens the risk of improper use and underscores the need for judicial supervision.

---

and adoption of the Fourth Amendment."); Boyd v. United States, 116 U.S. 616, 624–25 (1886) ("In order to ascertain the nature of the proceedings intended by the fourth amendment to the constitution under the terms 'unreasonable searches and seizures,' it is only necessary to recall the contemporary or then recent history of the controversies on the subject, both in this country and in England. The practice had obtained in the colonies of issuing writs of assistance to the revenue officers, empowering them, in their discretion, to search suspected places for smuggled goods, which James Otis pronounced 'the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book;' since they placed 'the liberty of every man in the hands of every petty officer.'").

[98] *See, e.g.*, Kelly, *supra* note 55 ("Law enforcement sources said the device sold to police is not set up to intercept content of calls or texts.").

[99] Gallagher, *supra* note 10 ("Procurement documents indicate that the Stingray can also be used with software called 'FishHawk,' (PDF) which boosts the device's capabilities by allowing authorities to eavesdrop on conversations. Other similar Harris software includes 'Porpoise,' which is sold on a USB drive and is designed to be installed on a laptop and used in conjunction with transceivers—possibly including the Stingray—for surveillance of text messages.").

[100] *Active GSM Interceptor: IBIS II - In-Between Interception System - 2nd Generation*, ABILITY, http://www.interceptors.com/intercept-solutions/Active-GSM-Interceptor.html (last visited Aug. 11, 2014).

[101] *IBIS (In-Between Interception System) Product Description*, ABILITY 4, *available at* http://toplinkpac.com/pdf/IBIS_Brochure.pdf.

[102] *Active GSM Interceptor: IBIS II - In-Between Interception System - 2nd Generation*, *supra* note 100.

III. The Fourth Amendment Framework

Two sometimes overlapping legal frameworks govern electronic surveillance by law enforcement officers: the Fourth Amendment of the U.S. Constitution, which protects against unreasonable searches and seizures, and the Electronic Communications Privacy Act ("ECPA"), which establishes legal requirements for government use of or access to wiretaps, pen registers, and electronic communications.[103] To qualify for protection under the former, the government action must first constitute a search or seizure, at which point law enforcement officers must obtain a warrant based on probable cause of criminal wrongdoing.[104] To qualify under the latter, government action must be of the kind specifically detailed in the statute, even if the action would not qualify as a search under existing caselaw.[105]

This Paper argues that the use of an ACSS is a Fourth Amendment search necessitating a warrant supported by probable cause. The government, however, almost uniformly rejects this contention, choosing instead to classify location information and ACSS operations, when discussed at all, as authorized by ECPA.[106] The two sections of ECPA currently used by law enforcement officials to obtain location and identifying information—the Stored Communications Act ("SCA") and the Pen Register/Trap and Trace Act ("PR/TT")—both allow the government to collect non-content consumer information from telecommunications carriers with showings of less than probable cause.[107] As a result, recognizing Fourth Amendment restrictions on ACSS operations would automatically disallow the government from seeking ECPA authority. A thorough examination of ECPA and other government arguments of statutory authority thus exceeds the scope of this Paper.

The Fourth Amendment ensures "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[108] What constitutes a search or seizure

---

[103] Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[104] *See* Kyllo v. United States, 533 U.S. 27, 32 (2001) (stating the Court's doctrine "that warrantless searches are presumptively unconstitutional"); United States v. Karo, 468 U.S. 705, 714–15 (1984) ("Searches and seizures inside a home without a warrant are presumptively unreasonable absent exigent circumstances."); Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."). *But see* California v. Acevedo, 500 U.S. 565, 582–83 (1991) (Scalia, J., concurring in judgment) (discussing how "the 'warrant requirement' had become so riddled with exceptions that it [is] basically unrecognizable").

[105] *See* United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979); Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 381–82 (2014) (describing how Congress was motivated by concerns about the lack of legal protections for information created by new computing technologies). *See also infra* Part III.D.

[106] *See infra* Part IV. The government hinges its statutory authority on sections of the Stored Communications Act, which covers law enforcement access to stored electronic and wire communications content and records, 18 U.S.C. §§ 2701–2712 (2012), and the Pen Register Act, which covers devices that records outgoing and incoming "dialing, routing, addressing, or signaling information" respectively, 18 U.S.C. §§ 3121–3127 (2012).

[107] 18 U.S.C. § 2703(c)(1) (allowing courts to issue orders for data covered by the Stored Communications Act upon proof of "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought[] are relevant and material to an ongoing criminal investigation"); 18 U.S.C. § 3122(b)(2) (requiring courts to allow law enforcement to install pen registers or trap and trace devices upon certification that "the information likely to be obtained is relevant to an ongoing criminal investigation").

[108] U.S. CONST. amend. IV.

turns on two complementary[109] paradigms: whether the government physically intruded upon an individual's house, papers, and effects ("trespass paradigm"),[110] or whether the government has violated "an actual (subjective) expectation of privacy . . . that society is prepared to recognize as 'reasonable'" ("privacy paradigm").[111]

A. *Jones* and the Dual Fourth Amendment Paradigms

Prior to 1967, Fourth Amendment jurisprudence required the government to physically trespass on the property of the defendant before classifying the behavior as a protected search.[112] In the seminal 1967 *Katz* decision, the Supreme Court overturned the predominance of the trespass paradigm, stating that "the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[113] Instead, the *Katz* Court found that the government's electronic surveillance of the defendant's conversation in a public telephone booth "violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[114] Justice Harlan's concurrence establishing the privacy paradigm's two-part test became the primary mechanism by which courts evaluated Fourth Amendment searches for the next five decades.[115]

After 45 years of dormancy, the trespass paradigm received new life in the Supreme Court's 2012 *Jones* decision. Operating outside the scope of the warrant, law enforcement officers attached a GPS device to a vehicle operated by the defendant and monitored his movements for 28 days.[116] Writing for the majority, Justice Scalia held that the installation of the GPS device and monitoring of Jones' location constituted a Fourth Amendment search because "[t]he Government physically occupied private property for the purpose of obtaining information."[117] In a footnote, Justice Scalia noted that this formulation is a two-part test: trespass to "persons, houses, papers, and effects" must be accompanied by "an attempt to find something or to obtain information" to qualify as a search.[118] Justice Scalia emphasized that "the Katz reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law

[109] "But as we have discussed, the Katz reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the commonlaw trespassory test." United States v. Jones, 132 S. Ct. 945, 952 (2012).
[110] *Id.* at 949 ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.' . . . We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").
[111] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
[112] *Compare* Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that a wiretap effected without physical trespass upon the defendants' property did not constitute a Fourth Amendment search) *with* Silverman v. United States, 365 U.S. 505, 512 (1961) (holding that surveillance conducted with a "spike mike" that physically intruded the defendants' home because it "is based upon the reality of an actual intrusion into a constitutionally protected area").
[113] Katz v. United States, 389 U.S. 347, 353 (1967).
[114] *Id.*
[115] *Id.* at 361 (Harlan, J., concurring). *See also* United States v. Jones, 132 S. Ct. 945, 949–50 (2012) (discussing the development of Fourth Amendment jurisprudence around the trespass and privacy paradigms).
[116] *Jones*, 132 S. Ct. at 948.
[117] *Id.* at 949.
[118] *Id.* at 951 n.5.

trespassory test."[119] As a result, situations not involving physical trespass "would remain subject to Katz analysis."[120]

Although a majority of justices in *Jones* upheld the continued relevance of physical trespass, a different but overlapping majority of justices also indicated that the Court would consider the cumulative effects of electronic surveillance that collects significant quantities of location information to violate a person's reasonable expectation of privacy ("REOP"). Justice Sotomayor joined the majority opinion, agreeing that a Fourth Amendment search occurs "at minimum" during a physical invasion by law enforcement.[121] Justice Sotomayor also agreed, however, with the concurrence in judgment written by Justice Alito, joining four other justices in recognizing that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[122] Dubbed the "mosaic theory," this view argues that even though each of one's movements over some period of time could be observed by law enforcement officials, the aggregate collection of that location information—and the related inferences born of those locational associations—impinges upon that person's REOP.

Despite their broad alignment under the mosaic theory, Justice Sotomayor and Justice Alito differed in their articulation of the privacy violation. Justice Alito condoned the "short-term monitoring" of an individual's movements on public streets without a warrant, citing *United States v. Knotts*,[123] but considered "lengthy monitoring"—for some period greater than "short-term" but lesser than four weeks—to cross a line into Fourth Amendment territory.[124] Society's expectation of privacy, he argued, "has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[125] Justice Sotomayor, by contrast, expressed concern about even short-term monitoring that would nevertheless allow the government to "generate[] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[126]

From a narrow perspective, *Jones* is remarkable only for reasserting that physical trespass constitutes a Fourth Amendment search—this is, after all, the majority's factual holding. Taken more broadly, however, *Jones* contains two important conclusions: first, that electronic surveillance conducted without physical trespass remains subject to the privacy paradigm; and second, that the Court will view with deep suspicion any government assertion that citizens lack an expectation of privacy in the aggregate collection of their movements.

B. The Privacy Paradigm in Location Tracking

Prior to *Jones*, the law of location tracking rested upon two Supreme Court cases from the mid-

[119] *Id.* at 952.
[120] *Id.* at 953.
[121] *Id.* at 954 (Sotomayor, J., concurring).
[122] *Id.* at 955 (Sotomayor, J., concurring) (internal citations omitted). *See id.* at 964 (Alito, J., concurring in judgment).
[123] *See infra* Part III.B.
[124] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in judgment).
[125] *Id.* (Alito, J., concurring in judgment).
[126] *Id.* at 955 (Sotomayor, J., concurring).

1980s that turned on the defendant's REOP or lack thereof. In the 1983 case *United States v. Knotts* (discussed previously in Part I), law enforcement officers warrantlessly placed a radio transmitter inside a chloroform container that was subsequently sold to and placed in the car of persons suspected of manufacturing illegal drugs.[127] Officers used visual surveillance and signals emanating from that transmitter to locate the suspects in a remote cabin and the container under a barrel outside.[128] The Court denied Fourth Amendment protection, finding that Knotts did not have a REOP in a car's movements on public highways nor in objects left in "open fields."[129]

A year later, the Court considered *United States v. Karo*, in which law enforcement officers likewise warrantlessly placed an electronic tracking device into a container of ether that was then sold to persons suspected of drug trafficking.[130] Government agents used the tracking device (but little visual surveillance) to monitor the container's location as it moved between several houses and storage facilities.[131] The Court distinguished *Knotts* and found that any electronic tracking device revealing information about the interior of the home constitutes a Fourth Amendment search.[132] Although the Court acknowledged that monitoring electronic tracking devices is less intrusive than a full-scale search, "it does reveal a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant"—namely, "that a particular article is actually located at a particular time in the private residence and is in the possession of the person or persons whose residence is being watched."[133] Critically, the Court rejected the government's complaint that under the Court's holding, the inability to know where suspects will travel while under the surveillance of a tracking device will force officers to obtain warrants in every case.[134] That a government surveillance method was so intrusive as to require a large number of warrants was "hardly a compelling argument against the requirement."[135]

Under *Knotts* and *Karo*, therefore, tracking devices implicate one's REOP when they reveal information not available to law enforcement officers through visual surveillance—in other words, information not knowingly exposed to the public. The possibility that *ex ante* ignorance about the suspect's potential non-public location will require law enforcement officials to seek many warrants before installing these devices is of little concern to the Court.

C. New Technology as a Fourth Amendment Search

The Court has also looked disapprovingly upon the government's warrantless use of new technology that allows the collection of information about the home's interior that would be otherwise unavailable without physical intrusion. In *Kyllo v. United States*, law enforcement officials stood on a public street and used a thermal imaging device to detect the infrared radiation levels emanating from

[127] United States v. Knotts, 460 U.S. 276, 278–79 (1983). *See also supra* Part I.
[128] *Id.* at 278–79.
[129] *Id.* at 282 (internal quotation marks omitted).
[130] United States v. Karo, 468 U.S. 705, 708 (1984).
[131] *Id.* at 708–10.
[132] *Id.* at 715.
[133] *Id.*
[134] *Id.* at 718.
[135] *Id.*

inside Kyllo's house.[136] The Court rejected arguments that the thermal imaging device only gleaned information "off the walls" of the home rather than "through the walls," (i.e., that the heat radiation was on the surface of the home and therefore did not require physical intrusion of residential walls), noting that such a mechanical approach would "leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home."[137] The Court also rejected a model that would differentiate between the obtainment of intimate and non-intimate details, observing that "[i]n the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes."[138]

Instead, the Court held that when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[139] In so holding, the Court operated primarily under the privacy paradigm, recognizing that the Fourth Amendment guarantees a reasonable expectation of privacy within the home.[140] Nevertheless, *Kyllo* also represents a middle ground between the trespass and privacy paradigms, equating certain technological intrusions as functionally equivalent to a physical intrusion conducted by a police officer.

D. The Third Party Doctrine Is Inapplicable to ACSS Operations

The Third Party Doctrine, emerging from two late-1970s Supreme Court cases, holds that individuals do not retain a REOP in documents or information voluntarily shared with third parties.[141] Although some members of the Court have indicated willingness to overturn or limit the Third Party Doctrine,[142] current Fourth Amendment jurisprudence continues to allow law enforcement officers unrestricted access to information voluntarily conveyed to anyone or anything else.[143]

Although the Third Party Doctrine haunts many of the government's electronic surveillance programs, the doctrine is uniquely inapplicable to an ACSS because the latter interacts directly with the target's cell phone. Unlike CSLI, which is collected by the third party telecommunications carrier, the location and identifying information obtained by an ACSS comes from the individual's cell phone, not a

[136] Kyllo v. United States, 533 U.S. 27, 29 (2001).
[137] *Id.* at 35–36.
[138] *Id.* at 37.
[139] *Id.* at 40.
[140] *Id.* at 34–35.
[141] Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding that the installation of a pen register to collect the outgoing telephone numbers dialed by Smith was not a search under the Fourth Amendment because Smith voluntarily conveyed the same information to the telephone company and therefore did not retain a REOP); United States v. Miller, 425 U.S. 435, 440–43 (1976) (holding that bank records concerning Miller's financial transactions were not subject to Fourth Amendment protection because they were the business records of the bank, not Miller's private papers, and because Miller had voluntarily revealed the information contained in the bank records to the third party bank and thus did not retain a REOP). *See also* Katz v. United States, 389 U.S. 347, 351 (1967) (denying Fourth Amendment protection to information "knowingly expose[d] to the public").
[142] *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").
[143] Law enforcement access to some information conveyed to third parties is restricted by means other than the Fourth Amendment, such as the Electronic Communications Privacy Act.

third party.

That the carrier possesses similar or even the same information does not invalidate the importance of this distinction. Under the Supreme Court's 2014 *Riley v. California* decision, law enforcement officers cannot review an arrestee's cell phone to determine what numbers he has recently dialed, despite their ability to obtain that same information, absent the Fourth Amendment's warrant requirement, from the arrestee's phone carrier.[144] Likewise, law enforcement officers cannot take a person's printed financial information off of her person without a warrant despite their ability to obtain the same information, absent Fourth Amendment protection, from her bank.[145] In other words, the Third Party Doctrine does not invalidate one's REOP in information shared with a third party *per se*; one's REOP vanishes only in the specific information shared with *and held by* that third party.

The ACSS represents perhaps the first time that law enforcement officials have been able to more easily obtain information from the targeted individual (by means of secrecy and duplicity) that they could otherwise collect legally from third parties. This results both from advancing technologies, which give law enforcement officers the means to conduct surveillance without third party involvement, and from the digital revolution, which has made it possible for the same information to be stored in multiple locations. Although a more nuanced discussion of the Third Party Doctrine in the digital age would certainly inform the debate surrounding government use of ACSSs, such discussion exceeds the scope of this Paper.

IV. Law Enforcement Duplicity Prevents Courts from Adequately Examining the Constitutional Implications of ACSS Operations

Despite at least two decades of use, few courts have grappled with the statutory and constitutional implications of ACSS operations. The handful of cases in which the government has explicitly acknowledged its use of cell site simulators fall into two categories: *ex post* analysis conducted in response to motions to suppress evidence obtained with the aid of a stingray, or *ex ante* analysis of government applications for court orders to authorize the use of a stingray.

Of the former, courts have either presumed that the government behavior was lawful or operated under a government stipulation that the stingray is a Fourth Amendment search. In *Thomas v. State*, law enforcement officers used a stingray to track a rape victim's phone to the home of the suspected perpetrator.[146] Although the defendant challenged the warrantless use of an ACSS, the court noted in a footnote that "we assume the police acted lawfully up to the point that they forcibly entered the apartment."[147]

---

[144] *See* Riley v. California, 134 S. Ct. 2473, 2492–93 (2014).
[145] By Fourth Amendment protection, I mean vis-à-vis the individual; the police still must comply with the Fourth Amendment and other laws when seeking information from the bank.
[146] Thomas v. State, 127 So. 3d 658, 659–60 (Fla. Dist. Ct. App. 2013). Law enforcement specifically avoided obtaining a search warrant and otherwise refused to disclose their use of a stingray because the department had signed a nondisclosure agreement with the manufacturer (most likely Harris Corporation). *Id.* at 660 ("An investigator with the technical operations unit of the Tallahassee Police Department . . . testified: 'We have not obtained a search warrant [in any case], based solely on the equipment.'"). *See* Wessler, *supra* note 70.
[147] *Thomas*, 127 So. 3d at 660 n.2.

In *United States v. Rigmaiden*, law enforcement officers obtained a warrant for the use of a mobile tracking device[148] to track the Verizon Wireless broadband air card used by an unidentified suspected fraudster.[149] According to Rigmaiden's allegations, which the government did not dispute, Verizon reconfigured the air card "so that it would connect to a fake cell site, or stingray, that the FBI was using to track his location."[150] Using a stingray, law enforcement officers tracked the air card to a specific unit in a California apartment complex.[151] During the extensive litigation that followed, the government conceded that use of an ACSS was a Fourth Amendment search and relied exclusively on the authorization provided by the tracking device warrant.[152]

In *State v. Tate*, law enforcement officers obtained a court order under the SCA, the PR/TT, the mobile tracking device statute, and Wisconsin state pen register/trap and trace laws to, *inter alia*, use a stingray to track a specific phone to the "south and east side of a particular apartment building."[153] The court "assume[d] without deciding" that the use of an ACSS constituted a search under both the Fourth Amendment and the Wisconsin Constitution, requiring a warrant.[154] The court then held that the search passed constitutional muster because law enforcement officers demonstrated probable cause, even though the government actually requested a court order (not a warrant) with a lower statutory showing requirement.[155] In addition, the court held that "[n]o specific statutory authority is necessary to the issuance of a valid warrant for cell site information."[156] In passing, the court noted that "law enforcement's use of a stingray to locate Tate's cell phone was reasonable."[157] Despite articulating an accurate description of ACSS operations,[158] the court's conclusion appears to assert—incorrectly—that

---

[148] Mobile tracking devices are "electronic or mechanical device[s] which permit[] the tracking of the movement of a person or object." 18 U.S.C. § 3117 (2012). Government use of tracking devices requires a warrant issued under Rule 41 of the Federal Rules of Criminal Procedure, FED. R. CRIM. P. 41(b)(4), (d)(1), (e)(2)(C), (f)(2), when the use of a tracking device implicates the Fourth Amendment, *see* H.R. Rep. 99–647, at 60 (1986) ("The section does not affect the legal standard for the issuance of orders authorizing the installation of each device. *See generally United States v. Karo*, 104 S. Ct. 3296 (1984) (a search warrant not required where the owner consents to installation); *United States v. Knotts*, 460 U.S. 276 (1983) (installation of a beeper on a container to follow on a public roadway does not violate the Fourth Amendment). The Court in Karo, *supra*, did find that if investigators used a beeper to determine whether the beepered object is in a private location, a warrant is required.").

[149] United States v. Rigmaiden, No. CR 08–814–PHX–DGC, 2013 WL 1932800, at *3, *14 (D. Ariz. May 8, 2013). "Air cards are devices that plug into a computer and use the wireless cellular networks of phone providers to connect the computer to the internet." Zetter, *supra* note 92.

[150] Zetter, *supra* note 92.

[151] *Rigmaiden*, 2013 WL 1932800, at *3.

[152] *Id.* at *15.

[153] State v. Tate, 849 N.W.2d 798, 802–04, 808 (Wis. 2014) (internal quotation marks omitted).

[154] *Id.* at 801.

[155] *Id.* at 809–10. *See* Cyrus Farivar, *Court Allows Use Of "Stingray" Cell Tracking Device In Murder Case*, ARS TECHNICA (July 24, 2014), http://arstechnica.com/tech-policy/2014/07/court-allows-use-of-stingray-cell-tracking-device-in-murder-case/ ("'[The court] talks a lot about there being probable cause but if the statutory authority was that used for a pen register, Wisconsin Statute 968.35 only requires a showing that evidence is "relevant to an ongoing criminal investigation" in order to use a pen register. That's not probable cause.'").

[156] *Tate*, 849 N.W.2d at 810–11.

[157] *Id.* at 811.

[158] *See id.* at 802 n.8 ("A stingray is an electronic device that mimics the signal from a cellphone tower, which causes the cell phone to send a responding signal. If the stingray is within the cell phone's signal range, the stingray measures signals from the phone, and based on the cell phone's signal strength, the stingray can provide an initial general location of the phone. By collecting the cell phone's signals from several locations, the stingray can develop the location of the phone quite precisely.").

the stingray acquired CSLI from Verizon rather than directly from the phone.[159]

Only two published opinions, both issued *ex ante*, have substantively addressed the legal impact of this new technology.[160] The first such case dates back to 1995 and involved a passive interception device called a "cellular phone digital analyzer," which could "detect the electronic serial number ('ESN') assigned to a particular cellular telephone, the telephone number of the cellular telephone itself, and the telephone numbers called by the cellular telephone."[161] Unable to identify by number the phones that it sought to surveil, the government instead applied for an order under the PR/TT "to analyze signals emitting from any cellular phone used by any one of five named subjects of a criminal investigation."[162]

The court first held that no court order of any kind was required prior to government use of a passive interception device because: (1) the information obtained by the digital analyzer fell outside of the Fourth Amendment due to the Third Party Doctrine, and (2) the PR/TT statute applied only to devices "attached" to phone lines.[163] The court then found that the PR/TT order for which the government had nevertheless applied[164] could not authorize the use of a passive interception device because the PR/TT, at the time, required law enforcement officers to identify the number that they sought to surveil.[165] Because law enforcement officers did not know the numbers of the suspects they sought to observe, such an open order could facilitate abuse and flout accountability. Indeed, the court expressed concern that "depending upon the effective range of the digital analyzer, telephone numbers and calls made by others than the subjects of the investigation could be inadvertently intercepted."[166]

The second case involved a law enforcement application for a PR/TT order to identify a suspect's phone number by operating a stingray for sixty days "at various locations in which the [Subject's] Telephone is reasonably believed to be operating."[167] Presuming without discussion that the government must obtain some form of court-issued authorization prior to operating the stingray, the court denied the PR/TT application for want of "a telephone number or some similar identifier."[168] The court further drew on the *Rigmaiden* case[169] to suggest, in *dicta*, that an ACSS qualified as a "mobile tracking device" and

[159] *Id.* at 811 ("According to Officer Brosseau's testimony, law enforcement officers tracked Tate's cell phone using cell site information obtained from a cellular service provider.").
[160] Several other opinions, not publically accessible, appear to deal with ACSS operations and have been collected and summarized by former Magistrate Judge Brian Owsley. Brian L. Owsley, *Triggerfish, Stingrays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 201–11 (2014).
[161] *In re* the Application of the US for an Order Authorizing Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197, 199 (C.D. Cal. 1995). The court noted in passing that the passive interception device in question could also be used to intercept cell phone conversation *content*, but that the government did not seek authorization to intercept content and would not have been authorized to collect content under the sought-after order anyway. *Id.*
[162] *Id.*
[163] *Id.* at 199–200. The court found upon brief analysis that the subjects retained no REOP in the numbers they dialed because individuals did not retain any REOP in dialed phone numbers under *Smith v. Maryland*. *Id.* at 199.
[164] "'[O]ut of an abundance of caution.'" *Id.* at 200.
[165] *Id.* at 201–02.
[166] *Id.* at 201.
[167] *In re* the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012) [hereinafter "*In re* Stingray"].
[168] *Id.* at 751.
[169] United States v. Rigmaiden, No. CR 08–814–PHX–DGC, 2013 WL 1932800 (D. Ariz. May 8, 2013).

conducted a Fourth Amendment search, thus requiring a warrant.[170]

Courts' limited analysis of ACSS operations belies their pervasive use among local, state, and federal law enforcement.[171] The lack of judicial review stems not from lack of contention but from systematic law enforcement pretense.[172] Rather than disclose ACSS operations, law enforcement officers frequently apply for court orders to install a "pen register/trap and trace device,"[173] or attribute ACSS-acquired location data to "information from a confidential source."[174] Many state and local police departments refuse to confirm whether or not they use ACSSs and deny public requests for information.[175] In June 2014, the U.S. Marshals even seized Florida State records responsive to an open records request to prevent their review by the American Civil Liberties Union.[176] Even the U.S. Senate

[170] *In re* Stingray, 890 F. Supp. 2d at 752.
[171] *See supra* notes 63–70 and accompanying text.
[172] *See, e.g.*, Jack Gillum, *Police Keep Quiet About Celltracking Technology*, ASSOCIATED PRESS (Mar. 22, 2014), https://news.yahoo.com/police-keep-quiet-cell-tracking-technology-070618821--finance.html; Jack Gillum & Eileen Sullivan, *US Pushing Local Cops To Stay Mum On Surveillance*, ASSOCIATED PRESS (June 12, 2014), http://finance.yahoo.com/news/us-pushing-local-cops-stay-174613067.html; Jenson & Bott, *supra* note 62; Maria Kayanan, *Internal Police Emails Show Efforts to Hide Use of Cell Phone Tracking*, ACLU (June 19, 2014), https://www.aclu.org/blog/national-security-technology-and-liberty/internal-police-emails-show-efforts-hide-use-cell; Linda Lye, *DOJ Emails Show Feds Were Less Than "Explicit" With Judges On Cell Phone Tracking Tool*, ACLU (Mar. 29, 2013), https://www.aclu.org/blog/national-security-technology-and-liberty/doj-emails-show-feds-were-less-explicit-judges-cell.
[173] 18 U.S.C. § 3122(b)(2) (requiring courts to allow law enforcement to install pen registers or trap and trace devices upon certification that "the information likely to be obtained is relevant to an ongoing criminal investigation"). *See* Tim Cushing, *Baltimore PD Hides Its Stingray Usage Under A Pen Register Order; Argues There's Really No Difference Between The Two*, TECHDIRT (Jan. 9, 2015), https://www.techdirt.com/articles/20150103/14461029590/baltimore-pd-hides-its-stingray-usage-under-pen-register-order-argues-theres-really-no-difference-between-two.shtml; Lye, *supra* note 172 (discussing internal DOJ emails that state in part: "It has recently come to my attention that many agents are still using [ACSS] technology in the field although the pen register application does not make that explicit."); Jennifer Valentino-Devries, *Sealed Court Files Obscure Rise in Electronic Surveillance*, WALL ST. J. (June 2, 2014), http://online.wsj.com/articles/sealed-court-files-obscure-rise-in-electronic-surveillance-1401761770 ("In 2011, magistrate judges in California complained that investigators were applying for pen registers without explicitly saying they wanted to use sophisticated cellphone-location trackers, called 'stingrays,' which can be used to locate suspects.").
[174] Cyrus Farivar, *Legal Experts: Cops Lying About Cell Tracking "Is A Stupid Thing To Do"*, ARS TECHNICA (June 20, 2014), http://arstechnica.com/tech-policy/2014/06/legal-experts-cops-lying-about-cell-tracking-is-a-stupid-thing-to-do/; Kayanan, *supra* note 172; Kim Zetter, *Emails Show Feds Asking Florida Cops to Deceive Judges*, WIRED (June 19, 2014), http://www.wired.com/2014/06/feds-told-cops-to-deceive-courts-about-stingray/.
[175] Gillum & Sullivan, *supra* note 172; Kelly, *supra* note 55; Eric Litke, *Wisconsin Department Of Justice Remains Mum On Cell-Tracking Surveillance*, GANNETT WIS. MEDIA (May 8, 2014), http://www.thenorthwestern.com/article/20140508/OSH0198/305080390 ("The state denied most of a public records request late last month seeking details on how often the device is used, how data is kept and shared, and how often warrants are obtained. Assistant Attorney General Kevin Potter wrote that such information 'could undermine law enforcement's ability to use investigative techniques . . . to effectively investigate criminal activity' and may violate homeland security regulations."); Lyndsay Winkley, *Why Cellular Tracking Device Is So Secret*, U-T SAN DIEGO (Dec. 22, 2014), http://www.utsandiego.com/news/2014/dec/22/stingray-cellular-tracking-police-documents/ ("The police department has said information about Stingrays is 'exempt from disclosure' [under public records laws] and in a statement Wednesday, the City Attorney's office said the Department of Justice directed no information to be released on the topic.")
[176] Nathan Freed Wessler, *U.S. Marshals Seize Local Cops' Cell Phone Tracking Files in Extraordinary Attempt to Keep Information From Public*, ACLU (June 3, 2014), https://www.aclu.org/blog/national-security-technology-and-liberty/us-marshals-seize-local-cops-cell-phone-tracking-files.

Committee on the Judiciary, charged with oversight of the FBI and the Department of Homeland Security, remains uninformed about federal law enforcement use of ACSS.[177]

Some law enforcement agencies justify their evasions by arguing that "criminals or terrorists could use the information to thwart important crime-fighting and surveillance techniques."[178] Other police departments deliberately conceal ACSS operations at the request of the U.S. Marshals Service, which is part of the Department of Justice,[179] or as a condition of acquiring an ACSS from the FBI.[180] And in several instances, law enforcement officers admitted that non-disclosure agreements signed with ACSS production companies prevented officers from revealing the existence of their stingray to anyone—including the courts.[181]

Law enforcement duplicity undermines the principle of judicial review, the foundation of the American legal system. The Federal Rules of Civil Procedure require that all parties before any court certify that "the factual contentions have evidentiary support"; any party that violates this rule is subject to court-imposed sanctions.[182] Courts must receive full information from the government if they are to fulfill their constitutional role as a check on legislative and executive power. By failing to provide candid information about their use of ACSSs, law enforcement agencies prevent judges from issuing honest opinions and subvert the constitutional balance of power between the government and its citizenry.

V. ACSS Operations Constitute a Fourth Amendment Search under the Trespass Paradigm

Due to law enforcement concealment of ACSS operations, no court has clearly determined

[177] Letter from Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary, & Sen. Charles Grassley, Ranking Member, S. Comm. on the Judiciary, to Eric Holder, Attorney General, Dep't of Justice, & Jeh Johnson, Sec'y of Homeland Sec., Dep't of Homeland Security (Dec. 23, 2014), *available at* https://www.leahy.senate.gov/download/12-23-14-pjl-and-ceg-to-doj-and-dhs1 [hereinafter "Judiciary Committee Letter"].

[178] Kelly, *supra* note 55. *See* Craig Timberg, *FBI Gags State and Local Police on Capabilities of Cellphone Spy Gear*, WASH. POST (Sept. 23, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/23/fbi-gags-state-and-local-police-on-capabilities-of-cellphone-spy-gear/ ("The bureau has said elsewhere that it considers the tactics used by IMSI catchers to be sensitive technology that could be defeated if too much information becomes available about its capabilities."); Adam Wagner, *WPD's Use of Cellphone Monitoring Gear Concerns Public Defender*, STAR NEWS ONLINE (June 19, 2014), http://www.starnewsonline.com/article/20140619/ARTICLES/140619615/-1/topic11?p=2&tc=pg.

[179] Zetter, *supra* note 174.

[180] Timberg, *supra* note 178 (reporting that a recent Freedom of Information Act request revealed FBI correspondence with a local police department stating "that the Federal Communications Commission authorizes the sale of [ACSS] equipment to state and local police departments on the condition that they first sign an FBI 'non-disclosure agreement'").

[181] Cyrus Farivar, *Prosecutors Drop Key Evidence At Trial To Avoid Explaining "Stingray" Use*, (Nov. 18, 2014), http://arstechnica.com/tech-policy/2014/11/prosecutors-drop-key-evidence-at-trial-to-avoid-explaining-stingray-use/ ("But rather than disclose the possible use of a stingray, also known as a cell site simulator, Detective John L. Haley cited a non-disclosure agreement, likely with a federal law enforcement agency (such as the FBI) and/or the Harris Corporation, since the company is one of the dominant manufacturers of such devices."); Jenson & Bott, *supra* note 62; Wessler, *supra* note 70 ("As two judges noted during the oral argument, as of 2010 the Tallahassee Police Department had used stingrays a staggering 200 times without ever disclosing their use to a judge to get a warrant.").

[182] FED. R. CIV. P. 11(b)(3), (c).

whether government use of an ACSS constitutes a search under the Fourth Amendment. In the absence of clear judicial guidance, this Part argues that ACSS operations by the government constitute a Fourth Amendment search because the device emits radio signals that conduct a physical trespass into a person's home and effects. Part VI then examines how ACSS operations also constitute a Fourth Amendment search under the privacy paradigm by violating the public's reasonable expectations of privacy.

All cellular devices operate using radio signals.[183] Radio signals, like all other types of light, are a form of electromagnetic radiation.[184] Although without mass,[185] radio signals carry energy and function as both particles and waves.[186] Due to their long wavelengths, radio signals can pass through walls and other physical obstacles.[187] When radio signals reach a receiving antenna, however, they accelerate electrons[188] in the antenna, creating an electric current that devices such as cell phones and televisions translate into sound and pictures.[189] Radio signals constitute the foundation upon which much of modern life is built, meaning that individuals in a reasonably developed city will be surrounded by thousands of radio signals at any one time.[190] Because of the many and varied uses for radio, different radio signals use different wave frequencies[191] so as to not interfere with each other or with other devices.[192]

The revival of the trespass paradigm requires courts to situate the radio signals emitted by an ACSS within common law property and tort doctrine, which has traditionally differentiated between trespass to land and trespass to moveable objects. Somewhat surprisingly, the Supreme Court's decision in *Jones* instead employed a more casual understanding of trespass law, suggesting a divergence between trespass actionable under common law and trespass actionable under the Fourth Amendment. The following Part first establishes the basic elements of trespass law, then examines how ACSS operations constitute a search under the trespass paradigm test established by the Supreme Court in *Jones*. This Part then looks more closely at the common law rationales underscoring modern trespass by so-called "intangible" objects to argue that ACSS operations also fit comfortably into more traditional common law tort doctrines.

---

[183] Blaze Testimony, *supra* note 25.
[184] JOHN D. CUTNELL & KENNETH W. JOHNSON, ESSENTIALS OF PHYSICS 499 (2006).
[185] Mass is a measurement of "the amount of matter contained in an object." JAMES TREFIL & ROBERT M. HAZEN, PHYSICS MATTERS 666 (2004). Mass is different than weight, which is the measure of the force of gravity. *Id.* at 100.
[186] Science Mission Directorate, *Anatomy of an Electromagnetic Wave*, NAT'L AERONAUTICS AND SPACE ADMIN., http://missionscience.nasa.gov/ems/02_anatomy.html (last visited Sept. 1, 2014).
[187] TREFIL & HAZEN, *supra* note 185, at 404.
[188] An electron is a subatomic particle that helps make up an atom. *Id.* at 449. Unlike electromagnetic radiation, electrons have mass. *Id.*
[189] *Id.* at 403–04; CUTNELL & JOHNSON, *supra* note 184, at 501.
[190] Marshall Brain, *How the Radio Spectrum Works*, HOW STUFF WORKS, http://electronics.howstuffworks.com/radio-spectrum.htm (last visited Sept. 1, 2014) (listing a number of wireless technologies that rely on radio signals, including garage door openers, cordless phones, cell phones, baby monitors, air traffic control radar, GPS, and television); Marshall Brain, *How Radio Works*, HOW STUFF WORKS, http://electronics.howstuffworks.com/radio3.htm (last visited Sept. 1, 2014).
[191] For example, FM radio operates at frequencies between 88 and 108 megahertz on the dial, and television channels 2–6 operate at frequencies between 58 and 88 megahertz. CUTNELL & JOHNSON, *supra* note 184, at 500.
[192] *See* OFFICE OF ENGINEERING AND TECHNOLOGY, FED. COMMC'N COMM'N, FCC ONLINE TABLE OF FREQUENCY ALLOCATIONS (2014) (listing the international and American allocation of radio frequencies).

A. A Brief Overview of the Common Law Trespass Framework[193]

Trespass law protects an owner's right to exclusive possession of her property. Two principle forms of trespass exist at common law: trespass *quare clasum fregit* and trespass to chattel. The former, otherwise known as trespass to land, consists of intentionally "enter[ing] land in the possession of the other, or caus[ing] a thing or a third person to do so," remaining on the land, or failing to remove a thing from the land.[194] To recover for trespass to land requires no showing of actual harm; a disruption in the property owner's right to exclusive possession of the property suffices.[195] Trespass to chattel covers "movable or transferable property"[196] and involves either "dispossessing another of the chattel" or "using or intermeddling with a chattel in the possession of another."[197] Unlike trespass to land, however, recovery requires the defendant to have caused actual injury (e.g., dispossession, damage to the object, loss of use, bodily harm, or harm to "thing in which the possessor has a legally protected interest").[198]

B. ACSS Operations Satisfy *Jones'* Conception of the Fourth Amendment Trespass Paradigm

In *Jones*, the Supreme Court considered whether the warrantless placement of a GPS device on Jones' car and subsequent month-long tracking violated the Fourth Amendment.[199] Operating under the trespass paradigm, the Court held that simply placing a GPS device on Jones' vehicle—a legal piece of chattel—and using it to monitor the vehicle's movements constituted a Fourth Amendment trespass because it "physically occupied private property for the purpose of obtaining information."[200] Despite the established common law doctrine requiring a showing of harm when a "tangible" object trespasses on moveable objects, neither the majority opinion nor the two concurrences discussed the absence of—or a need for—actual harm to the vehicle or to Jones' use of it.[201] Instead, both Justice Scalia and Justice Sotomayor found that mere "physical intrusion" for the purpose of obtaining information constitutes a Fourth Amendment search.[202]

Government operation of an ACSS constitutes such a Fourth Amendment search because an

---

[193] This Paper focuses on federal constitutional law but requires analysis of property and tort law, fields primarily relegated to the states. To avoid a hairy exploration of the different property and tort doctrines of the many states, this Paper adopts widely accepted principles of tort and property law as expressed in the Restatement (Second) of Torts and the Restatements (Third) of Torts: Physical and Emotional Harm, with reference to some cases that serve as exemplars of widely-adopted doctrines. Different state tort and property doctrines thus exceed the scope of this Paper. More fundamentally, differences between the states in the interpretation and application of tort and property law exceed the scope of any analysis of Fourth Amendment protection, which should not vary depending on the state in which the government search takes place.

[194] RESTATEMENT (SECOND) OF TORTS § 158 (1965). *See also* RESTATEMENT (THIRD) OF TORTS: PHYS. & EMOT. HARM § 50 (2012) ("A trespasser is a person who enters or remains on land in the possession of another without the possessor's consent or other legal privilege.").

[195] MARK A. GEISTFELD, ESSENTIALS TORT LAW 130–31 (2008).

[196] BLACK'S LAW DICTIONARY 251 (8th ed. 2004).

[197] RESTATEMENT (SECOND) OF TORTS § 217.

[198] *Id.* § 218. *See* GEISTFELD, *supra* note 195, at 131–32.

[199] United States v. Jones, 132 S. Ct. 945, 948 (2012).

[200] *Id.* at 949.

[201] Justice Alito does mention, however, that placing the GPS on a car "is generally regarded as so trivial that it does not provide a basis for recovery under modern tort law." *Id.* at 961 (Alito, J., concurring in judgment).

[202] *Id.* at 949; *id.* at 954 (Sotomayor, J., concurring).

ACSS uses radio signals to physically intrude individuals' property for the purpose of obtaining information. An ACSS easily satisfies the second prong of the Court's test: the sole function of an ACSS is to obtain the identifying and location information of cell phones. An ACSS also satisfies the first prong because it actively sends radio signals that physically intrude upon individuals' homes and effects.[203]

Radio signals carry substantial amounts of data and produce both passive and active changes in traditional "tangible" items. Modern technology uses radio signals to open garage doors, operate remote-controlled cars and drones, connect laptops and smartphones to the Internet, and project music, voices, and images on radios, televisions, and cell phones.[204] The changes occur due to the current created in the receiving antenna by the radio signals.[205] The visible manifestation of this current proves that the radio signals have perpetrated physical contact: had the signals not "touched" the garage door, television, or cell phone, that object would not have opened, displayed programming, or rang (respectively). For the garage door to open, therefore, the radio signals must emanate from the controller and interact with the door. Indeed, most modern electronics—cell phones included—*only* have value because of the physical changes caused by radio signals. More precisely, we value electronic devices because they provide the ability to *exclusively* control physical changes via radio signals. Modern society would be much less likely to embrace new technologies if we expected strangers to have the ability to change our TV channels or open our garage doors without permission.

ACSS operations interfere with one's exclusive control of her cell phone. The device "touches" a cell phone via radio signals, forcing it to operate at maximum power,[206] register with the device, and hand over identifying and location information. An ACSS can even disrupt the user's wireless connection.[207] Absent the device's active intrusion, the law enforcement official operating the ACSS would not have changed the phone's tower registration and obtained the user's data. Therefore, an ACSS—like a larger GPS device—physically intrudes on individuals' private effects. Combined with their intrinsic information-gathering function, ACSS operations constitute a Fourth Amendment search under the trespass paradigm articulated in *Jones*.

C. A Common Law Trespass Paradigm Bars Warrantless ACSS Operations

By expanding the scope of trespass necessary to trigger Fourth Amendment protection without upsetting property and tort law across the country, the Supreme Court appears to create a distinction between a trespass actionable under the Fourth Amendment and a trespass actionable under tort law.[208] Under this new paradigm, ACSS operations constitute a Fourth Amendment search by committing a *Fourth Amendment* trespass, defined as physical intrusion plus intent to gather information, regardless of common law harm requirements. Whether this paradigm will carry forward into future Fourth

[203] State v. Tate, 849 N.W.2d 798, 822 (Wis. 2014) (Abrahamson, C.J., dissenting).
[204] *See supra* note 190.
[205] *See supra* note 189.
[206] Hruska, *supra* note 61.
[207] United States v. Rigmaiden, No. CR 08–814–PHX–DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013) ("The mobile tracking device caused a brief disruption in service to the aircard.").
[208] *See* James Grimmelmann, *The Fourth Amendment and the Common-Law Trespass Torts*, TECH. | ACADEMICS | POLICY (TAP) (June 21, 2012), http://www.techpolicy.com/Grimmelmann_FourthAmendment-and-Common-LawTrespassTorts.aspx.

Amendment jurisprudence, however, remains uncertain. In the absence of clear judicial embrace of this trespass binary, this Paper argues for a theory of radio signal trespass consistent with existing common law.

A problem arises, however, because applying traditional trespass law to radio signals is fundamentally impracticable. Radio signals form the foundation of modern society, with thousands of signals permeating private property at any one time. Allowing pure physical intrusion by radio signals to be an actionable tort would invite trespass suits against radio and television stations, baby monitors, remote controlled vehicles, and garage door openers. Indeed, objects emitting signals along the whole electromagnetic spectrum, including front porch lights, body heat, and x-ray machines, would become litigation fodder. Prudent Fourth Amendment jurisprudence should not risk expanding the scope of trespass to swallow all forms of signal intrusion.

At the same time, a fundamental difference exists between sending radio signals throughout a city that passively disseminate information to anyone who chooses to intercept them (e.g., radio stations) or sending radio signals that produce a beneficial effect to which the property owner consents (e.g., garage door openers), and sending radio signals throughout a city that actively intrude upon physical devices, without the owner's consent, to steal identifying and location information. In addition, the problem of radio signals is not limited to ACSSs; rapidly advancing digital technology will provide the government with an ever-increasing arsenal of tools that use electromagnetic radiation to gain information from persons, houses, papers, and effects.

An effective Fourth Amendment trespass paradigm must prohibit government operation of invasive wireless technologies (without a warrant) while both operating within existing tort and property jurisprudence and not harming the many forms of wireless technology that underpin society. Under the proposed rule, a physical intrusion by electromagnetic radiation (including radio signals) would only qualify as trespass if: (i) the operator of the device producing electromagnetic radiation intended to intrude on the property of another; (ii) the owner of the property did not consent to the intrusion; and (iii) the electromagnetic radiation actively produced a physical change in the intruded-upon property. Each prong will be discussed in turn.

i. Intent

The first prong allows a cause of action for trespass by radio signals only if the operator *intended* to intrude on the property of another. Intent is central to the most widely used forms of trespass to land and trespass to chattel.[209] The second and third restatements of tort law define intent as a desire to cause

[209] RESTATEMENT (SECOND) OF TORTS § 158 ("One is subject to liability to another for trespass . . . if he *intentionally* (a) enters land in the possession of the other, or causes a thing or a third person to do so, or (b) remains on the land, or (c) fails to remove from the land a thing which he is under a duty to remove." (emphasis added)); *id.* § 217 ("A trespass to a chattel may be committed by *intentionally* . . . ." (emphasis added)).

Although trespass to land and trespass to chattel are most commonly viewed as intentional torts, tort law does create causes of action for reckless or negligent forms of trespass. For example, a plaintiff can recover for intrusions to real property caused by reckless or negligent conduct and abnormally dangerous activities, provided that the intrusion causes harm. *Id.* § 165. The old common law doctrine of trespass on the case further allows a cause of action for

the consequences of an act or the belief that the consequences are substantially certain to result from it.[210] In other words, intent covers both desired and undesired consequences, provided that the trespasser is substantially certain that the latter will result from her actions.[211] As a result, this prong prevents the application of trespass law to cell phones, x-ray machines, baby monitors, and garage door openers whose operators do not intend to intrude on others' property and cause an active physical change (see Part V.C.iii below). The prong does extend trespass liability, however, to government uses of ACSS that obtain identifying and location information from persons other than the intended target (see Part II.C.ii above). A rational operator of ACSS knows, if not intends, that the device will forcibly connect with all phones in the vicinity in order to transmit identifying and location information.

ii. Absence of Consent

Consent is an inherent part of property and tort law. If a party consents to the actions of another who intrudes upon her legally protected interests, she cannot recover.[212] Rigorously enforcing the absence of consent prong will eliminate the risk of trespass law applying to radio and television stations, cell phone companies, x-ray machines, and owners of baby monitors and garage doors. Not only can these signals not actively change property (see Part V.C.iii below), but one can only be exposed to the effects of these signals by purchasing and activating the relevant device—in other words, giving consent.

Crucially, the trespass-mitigating function of consent is limited only to the person or entity to which consent is granted. Just as allowing a friend on your property does not allow all other human beings on your property, allowing a telecommunications carrier to access your cell phone to provide signal and related services does not allow everyone else unrestricted access to your phone and its contents.

Acknowledging the importance of consent is also consistent with the Supreme Court's most recent decision addressing the Fourth Amendment and trespass. In *Florida v. Jardines*, two police officers brought a drug-sniffing dog to a homeowner's porch where it signaled the presence of marijuana.[213] The Court held that the police dog transformed the officers' behavior into a protected search.[214] Operating under the trespass paradigm, the Court recognized an implicit license to approach a stranger's home and

---

"indirect or consequential harms." City of Monterey v. Del Monte Dunes at Monterey, Ltd., 526 U.S. 687, 729 (1999) (Scalia, J., concurring in part and concurring in judgment). *See* Scheuering v. United States, No. 14-CV-932 NSR, 2014 WL 6865727, at *5 (S.D.N.Y. Dec. 4, 2014) ("Trespass on the case is an old common law cause of action, the purpose of which was to supply a remedy where the other forms of [trespass] actions were not applicable." (internal citation omitted)). More commonly, a plaintiff can always recover for damage to chattel caused by negligence. RESTATEMENT (SECOND) OF TORTS § 281 ("The actor is liable for an invasion of an interest of another, if: (a) the interest invaded is protected against unintentional invasion, and (b) the conduct of the actor is negligent with respect to the other, or a class of persons within which he is included, and (c) the actor's conduct is a legal cause of the invasion, and (d) the other has not so conducted himself as to disable himself from bringing an action for such invasion."). By contrast, purely accidental intrusions (unintentional and non-negligent) do not give rise to liability, *even if* the intrusion causes harm. *Id.* § 166.

[210] RESTATEMENT (THIRD) OF TORTS: PHYS. & EMOT. HARM § 1 (2010); RESTATEMENT (SECOND) OF TORTS § 8A.

[211] RESTATEMENT (SECOND) OF TORTS § 8A cmt. b.

[212] RESTATEMENT (SECOND) OF TORTS § 892A(1) (1979).

[213] Florida v. Jardines, 133 S. Ct. 1409, 1413 (2013).

[214] *Id.* at 1417–18 ("The government's use of trained police dogs to investigate the home and its immediate surroundings is a 'search' within the meaning of the Fourth Amendment.").

knock but found that the introduction of a police dog exceeded the scope of the license.[215] This implicit license of consent prevents a Fourth Amendment trespass paradigm involving radio signals from grossly expanding tort law. Under the implicit license of consent, people are free to call or email strangers[216] but not free to, for example, hack into their computers to obtain information.

iii. Active Intrusion Causing a Physical Change

The traditional view of trespass requires the trespass to be conducted by tangible objects, seemingly defined as objects larger than grains of dust.[217] Traditional tort law thus relegates physical intrusion by so-called "intangibles" such as dust, noise, and electronic signals to the law of nuisance.[218] Nuisance involves a substantial, unreasonable, and non-trespassory interference in one's free use and enjoyment of property that results in actual injury.[219] Nuisance law, however, is wholly inapplicable to the radio signals issued by an ACSS. First, nuisance law applies to interferences with land, not with chattel. Second, as with the GPS device in *Jones*, government use of ACSSs does not typically interfere with an individual's use and enjoyment of her cell phone.[220] Instead, an ACSS directly intrudes upon the individual's right to exclusive possession of her phone and the location and identifying information it contains—an interest designed to be protected by trespass.

The modern view of trespass to land, by contrast, recognizes that intrusion by seemingly invisible particles can constitute physical trespass—provided that the intrusion causes tangible damage.[221] Unlike "tangible" objects, the courts presume that "invasions by intangibles such as light or sound will not always interfere with the person's rights of possession."[222] Demonstrating harm, therefore, proves that the property owner has suffered an interference with her right to exclusive possession and avoids an unnecessary expansion of trespass law.[223] In a parallel line of cases, some courts have recognized that

---

[215] *Id.* at 1416.

[216] *See* Intel Corp. v. Hamidi, 71 P.3d 296, 300, 311 (2003) (rejecting, *inter alia*, a request to transplant traditional trespass law to electronic communications out of fear that such a doctrine would "create substantial new costs, to e-mail and e-commerce users and to society generally, in lost ease and openness of communication and in lost network benefits"). Through the *Jardines* lens, this policy decision can be understood as protecting the implicit license to operate on other people's property to send communications.

[217] Adams v. Cleveland-Cliffs Iron Co., 602 N.W.2d 215, 219 (1999).

[218] *See, e.g.*, Campbell v. Seaman, 63 N.Y. 568, 577 (1876) (finding that the defendant's production of gas that intruded upon the plaintiff's property constituted a nuisance).

[219] *See* Hendricks v. Stalnaker, 380 S.E.2d 198, 200 (W.V. 1989) ("[W]e define a private nuisance as a substantial and unreasonable interference with the private use and enjoyment of another's land. The definition of private nuisance includes conduct that is intentional and unreasonable, negligent or reckless, or that results in an abnormally dangerous conditions or activities in an inappropriate place."); RESTATEMENT (SECOND) OF TORTS § 821.

[220] An ACSS does, however, force cell phones to operate at maximum power and can disrupt the user's wireless connection. *See supra* notes 206–207 and accompanying text.

[221] *See, e.g.*, *In re* WorldCom, Inc., 546 F.3d 211, 217 (2d Cir. 2008) (listing cases from Alaska, Colorado, and Washington that have adopted the modern view, and predicting that the Kansas Supreme Court, if it recognized trespass by intangible objects, would adopt the modern view); *Cleveland-Cliffs Iron Co.*, 602 N.W.2d at 219–21 (detailing courts that have adopted the modern view, but ultimately declining to so adopt because the associated requirement of damages by the intangible objects, adopted by other courts, blurs the line between trespass and nuisance).

[222] In re *WorldCom, Inc.*, 546 F.3d at 218–19 ("By contrast, invasions by intangibles such as light or sound will not always interfere with the person's rights of possession—unless there is substantial damage to the res.").

[223] *Id.*

electronic signals constitute a tangible intrusion to *chattel*.[224] As with all trespasses to chattel claims, the plaintiff must demonstrate actual injury to recover. The harm requirement exists because in traditional circumstances, a property owner's right to exclusive possession of his property is adequately protected by "his privilege to use reasonable force to protect his possession against even harmless interference."[225] As a result, emerging common law concerning intrusion by microscopic or atomic particles has evaporated the traditional distinction between trespass to chattel and trespass to land, allowing a claim of trespass to move forward upon adequate showing of injury by "intangible" objects.

These two policy rationales underlying the need for a showing of harm—the need for certain proof that the property owner has suffered an interference with her right to exclusive possession, and the assumption that moveable property owners can use self-help to prevent intrusions—are not relevant when considering an ACSS. When an ACSS actively interacts with cell phones, it does not interfere with the phone's functionality and therefore does not cause physical harm in the modern legal sense.[226] Instead, these devices actively and physically interfere with phones by forcing them to register with the stingray and reveal identifying and location information. This active intrusion and consequent physical change will *always* violate a cell phone owner's right to exclusive possession of her cell phone. In addition, because an ACSS operates in secret and leaves no trace of the intrusion, cell phone owners are unable to take protective measures to shield their chattel from even "harmless" intrusion.[227]

The third prong would, therefore, require that the physical intrusion, in addition to being intentional and nonconsensual, actively produce a physical change in the offended property. This prong serves as a proxy for the common law requirement of harm, which itself had served as a proxy for claims worthy of legal protection. Requiring active intrusion producing a physical change prevents common radio signal transmissions (such as television and radio broadcasts) and other forms of electromagnetic radiation (such as body heat, front porch lights, and x-rays) from qualifying as trespass. A radio broadcast simply transmits music and speech; radio broadcasts cannot turn on a person's radio, adjust the dial, or take personal information back to the station. Garage door opens, by contrast, do actively produce a physical change—opening a garage door—and so would trigger trespass liability under this test; indeed, good policy dictates that intentionally opening someone else's garage door without her consent *should* qualify as trespass.

Such a rule, besides correctly targeting only that behavior which *should* constitute a trespass in the digital age, protects the privacy interests that underpin property law.[228] Privacy is "the condition or

---

[224] *See, e.g.*, Intel Corp. v. Hamidi, 71 P.3d 296, 304–06 (Cal. 2003) (discussing the development of electronic signal trespass to chattel doctrine); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1020–23 (S.D. Ohio 1997) ("Electronic signals generated and sent by computer have been held to be sufficiently physically tangible to support a trespass cause of action."); Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 & n.6 (Cal. Ct. App. 1996) ("In our view, the electronic signals generated by the Bezenek boys' activities were sufficiently tangible to support a trespass cause of action.").

[225] RESTATEMENT (SECOND) OF TORTS § 218, Comment e. *See* GEISTFELD, *supra* note 195, at 132.

[226] *Hamidi*, 71 P.3d at 304–06 (reviewing similar cases in other courts that recognized harm when the trespass "actually did, or threatened to, interfere with the intended functioning of the system, as by significantly reducing its available memory and processing power").

[227] To suggest that cell phone owners simply turn off cell phones, or switch them to airplane mode, to avoid ACSS detention is like suggesting the owner of a Porsche dismantle the vehicle to prevent unwanted trespass.

[228] *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)

state of being free from public attention to intrusion into or interference with one's acts or decisions."[229] Freedom from intrusion is simply another way of framing the traditional justification of property: protecting the owner's right to exclusive use of her property and complementary right to exclude others from using her property.[230] As new technologies create new ways to violate one's rights of use and exclusion, property law must not abdicate its protective role simply because the intrusion occurs outside of traditional human experience. Likewise, the Fourth Amendment trespass paradigm must preserve constitutional protections against new technologies that allow for surreptitious physical intrusion into one's home and effects.

VI. ACSS Operations Constitute a Fourth Amendment Search under the Privacy Paradigm

Following the 1967 *Katz* decision, whether government behavior constitutes a search almost always turns on whether the government violated a person's reasonable expectation of privacy ("REOP").[231] The Court usually measures REOP by determining whether the subject possessed "an actual (subjective) expectation of privacy . . . that society is prepared to recognize as 'reasonable.'"[232] Courts measure reasonability using several different assessments of social recognition: whether the intrusion occurs frequently or routinely, whether the surveillance intrudes a constitutionally protected space, or whether the expectation of privacy should be preserved.

Despite the persistence of Justice Harlan's two-part text, the assertion that certain behavior violates a societal expectation of privacy is always fraught with evidentiary hurdles. Judges struggle to measure the aggregate feelings of some 300 million individuals and risk substituting their personal expectations for that of the average citizen.[233] Of even greater concern is circularity, by which judicial decisions claim to discern social expectations but actually *establish* new expectations by invalidating

---

(examining common law doctrines that provide protection for person and property to discern the modern right to privacy and its bounds).

[229] BLACK'S LAW DICTIONARY 1233 (8th ed. 2004).

[230] J.E. PENNER, THE IDEA OF PROPERTY IN LAW 75–76 (1997).

[231] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). *See also* United States v. Jones, 132 S. Ct. 945, 952 (2012) ("But as we have discussed, the Katz reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the commonlaw trespassory test.").

[232] *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Although a two-step analysis is well-established in legal precedent, Orin Kerr has recently argued that the subjective element of Justice Harlan's test has become a phantom: dutifully recited but never outcome determinative. Orin Kerr, *How "Subjective Expectations of Privacy" Became Irrelevant*, VOLOKH CONSPIRACY WASH. POST (July 3, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/07/03/how-subjective-expectations-of-privacy-became-irrelevant/. Professor Kerr argues that Justice Harlan intended the first prong of his test (the "subjective" test) to measure whether the defendant had waived his Fourth Amendment rights by exposing the information or location to the plain view of outsiders, while the second prong (the "objective" test) was intended to measure whether the defendant's information or location received Fourth Amendment protection to begin with. *Id.* Instead, Supreme Court jurisprudence has interpreted the subjective prong to measure whether a defendant believes that his location or information will be private, and combined Justice Harlan's two points into the objective prong, which now measures both whether the information or location receives Fourth Amendment protection and whether the defendant has waived that protection through knowing exposure. *Id.* Because the subjective prong is never outcome determinative (i.e., a person sitting in his home expecting the cops to burst through the door never loses Fourth Amendment protection), Professor Kerr argues that it should be eliminated. *Id.*

[233] *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 962 (Alito, J., concurring in judgment); Kyllo v. United States, 533 U.S. 27, 34 (2001).

those claimed by the parties.[234] Recognizing REOP, therefore, requires the Court to both explore how the surveillance method at issue affects contemporary understandings of privacy and determine whether society does (or should) recognize those expectations as valid.

Without conceding the viability of Fourth Amendment protections under the trespass paradigm, this Part will argue first that government use of ACSSs violates the public's subjective expectation of privacy and then situate ACSS operations within the varying measures of reasonability. This Part concludes by asserting that although ACSS operations violate socially recognized reasonability under both of the Court's traditional measurements, rapidly advancing technology mandates that courts separate legal privacy from secrecy and instead establish positive barriers around spheres that we as a society seek to preserve as private.

A. Individuals Have Subjective Expectation of Privacy in Their Identifying and Location Information

Under the *Katz* regime, a person loses REOP in whatever information she "knowingly exposes to the public."[235] By rational corollary, what an individual does *not* knowingly expose to the public or what she "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[236]

As discussed in Part II, cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[237] The vast majority of Americans own cell phones and have access to mobile phone networks.[238] Unlike Jones' car, Karo's container of ether, or Knotts' container of chloroform, however, we carry cell phones with us constantly. Cell phones lie next to our beds as we sleep, sit in our bags at work, stay in our pockets as we go about the business of our days, and remain close by when we return home. A cell phone's location is thus a proxy for the individual's location, with the potential to reveal "'trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.'"[239]

Because cell phones accompany individuals everywhere, these individuals subjectively retain an expectation of privacy in all personal information during those moments not knowingly exposed to the public or preserved as private. ACSS operations identify all nearby cell phone users, information about which individuals enjoy established constitutional protections in non-electronic circumstances.[240] They

[234] *See, e.g.*, *Kyllo*, 533 U.S. at 34 ("The Katz test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable.").
[235] Katz v. United States, 389 U.S. 347, 351 (1967).
[236] *Id.*
[237] Riley v. California, 134 S. Ct. 2473, 2484 (2014).
[238] FED. COMMC'N COMM'N, 16TH ANNUAL MOBILE WIRELESS COMPETITION REPORT, *supra* note 20, at 10, 28; Duggan, *supra* note 19.
[239] United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).
[240] Brown v. Texas, 443 U.S. 47, 50 (1979) ("When the officers detained appellant for the purpose of requiring him

also obtain location information from phones without regard to whether the phone's owner has knowingly disclosed that information to the public. All three cases in which the government admitted use of an ACSS resulted in law enforcement officers locating the phone in the constitutionally protected space of the home.[241] The collection of cell location information, therefore, "convert[s] what would otherwise be a private event into a public one,"[242] violating individual expectations of privacy. Indeed, in the absence of constitutional restrictions, and responding to public concern, a number of states have begun to enact positive protections for cell phone information.[243]

The development of smartphone applications that allow users to broadcast their identity and location to their friends, to Google,[244] or to the public does not undermine a subjective expectation of privacy in one's identity and location. A phone's ability to share location information with others is optional; users must download an application or enable the phone's location reporting services. Even users who do choose to share their location typically share with a select group of friends and family, not the public at large. That the Internet abounds with how-to articles to disable various tracking features on cell phones underscores the argument that privacy, not transparency, remains the default expectation.[245]

The American public's awareness of government surveillance also fails to negate the public's ability to retain a subjective expectation of privacy.[246] The widespread public outrage expressed in response to Edward Snowden's revelations of mass government surveillance indicate that the public still expects daily communications—and the identifying and location information that accompany them—to remain private. Indeed, public dissatisfaction with surveillance has pushed major corporations responsible for Americans' telecommunications activities to release transparency reports,[247] fight government court orders,[248] and push for stricter surveillance laws.[249]

---

to identify himself, they performed a seizure of his person subject to the requirements of the Fourth Amendment.").

[241] Thomas v. State, 127 So. 3d 658, 659–60 (Fla. Dist. Ct. App. 2013); United States v. Rigmaiden, No. CR 08–814–PHX–DGC, 2013 WL 1932800, at *3 (D. Ariz. May 8, 2013); State v. Tate, 849 N.W.2d 798, 803–04 (Wis. 2014). *See Jones*, 132 S. Ct. at 950 n.3 ("Where, as here, the Government obtains information by physically intruding on a constitutionally protected area, such a search has undoubtedly occurred.").

[242] United States v. Davis, 754 F.3d 1205, 1216 (11th Cir. 2014), *reh'g en banc granted, opinion vacated*, 573 F. App'x 925 (11th Cir. 2014).

[243] *See infra* note 312.

[244] *E.g.*, *Google Location History*, GOOGLE, https://maps.google.com/locationhistory/b/0 (last visited Sept. 7, 2014).

[245] *See, e.g.*, Kashmir Hill, *Change This iPhone Setting To Stop Closed Apps From Tracking Your Location*, FORBES (Aug. 11, 2014), http://www.forbes.com/sites/kashmirhill/2014/08/11/iphone-app-location-tracking/.

[246] *See, e.g.*, Ellen Nakashima, *NSA Had Test Project to Collect Data on Americans' Cellphone Locations, Director Says*, WASH. POST (Oct. 2, 2013), http://www.washingtonpost.com/world/national-security/nsa-had-test-project-to-collect-data-on-americans-cellphone-locations-director-says/2013/10/02/65076278-2b71-11e3-8ade-a1f23cda135e_story.html.

[247] *Comcast Issues First Transparency Report*, COMCAST (Mar. 20, 2014), http://corporate.comcast.com/comcast-voices/comcast-issues-first-transparency-report (revealing 24,698 subpoenas, court orders, and warrants for consumer data in 2013); *Transparency Report*, AT&T, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html (last visited Aug. 8, 2014) (revealing 115,925 subpoenas, court orders, and search warrants for consumer data in the first half of 2014); *Verizon's Transparency Report for the First Half of 2014*, VERIZON, http://transparency.verizon.com/us-report (last visited Aug. 8, 2014) (revealing 321,545 subpoenas, court orders, warrants, and emergency requests from law enforcement for consumer data in 2013).

[248] *See, e.g.*, Marcy Gordon & Martha Mendoza, *Telecom Giants Reportedly Join Tech Firms In Pushing Back Against NSA*, SAN JOSE MERCURY NEWS (Mar. 3, 2014), http://www.mercurynews.com/business/ci_25265560/telecoms-giants-reportedly-join-tech-firms-pushing-back.

[249] Edward Wyatt & Claire Cain Miller, *Tech Giants Issue Call for Limits on Government Surveillance of Users*,

Nor could Congressional legislation (e.g., a statute allowing short-term warrantless location tracking with ACSS) or Executive Branch activities and regulations (e.g., a notice and comment rulemaking[250] establishing procedures for the warrantless use of an ACSS) negate the public's subjective expectation of privacy. Congressional and executive actions remain subject to the Constitution as interpreted by the Supreme Court.[251] Congress and the Executive Branch cannot backdoor the absence of Fourth Amendment protection by informing the public about surveillance practices and then arguing that this awareness moots subjective expectations of privacy. Indeed, to allow otherwise would gut the Fourth Amendment, creating a perverse incentive for these branches to simply publicize (and even codify) ever more invasive forms of surveillance in order to evade Fourth Amendment protection.

Finally, the decision to purchase a cell phone does not indicate consent to warrantless law enforcement surveillance of the phone's identifying and location information.[252] Consent to search must be voluntary as determined by the totality of the circumstances, but the circumstances here signify otherwise.[253] First, cell phone contracts function like adhesion contracts, in which users have no ability to negotiate individual terms.[254] Given the importance cell phones play in modern life,[255] users should not be penalized for contracting on terms beyond their control. Second, cell phone companies do not publicize details concerning what information they collect from users and for how long they store it.[256] As a result, two federal circuit courts have decided that cell phone users do not voluntarily share their location information with cell phone companies.[257] Finally, even assuming that users are perfectly informed about what information the carriers collect and retain, this expectation of collection and retention extends to the carrier alone.[258] Allowing the government to collect the same information directly from the individual's phone, without a warrant, would be like law enforcement officers entering your home without a warrant because you gave your neighbor permission to water your plants while you were on vacation.

N.Y. TIMES (Dec. 9, 2013), http://www.nytimes.com/2013/12/09/technology/tech-giants-issue-call-for-limits-on-government-surveillance-of-users.html?pagewanted=all&_r=0.

[250] *See* 5 U.S.C. § 553 (2012) (describing the procedures for notice and comment rulemaking).

[251] *See* Dickerson v. United States, 530 U.S. 428, 437 (2000) ("But Congress may not legislatively supersede our decisions interpreting and applying the Constitution."); Marbury v. Madison, 5 U.S. 137, 180 (1803) ("[A] law repugnant to the constitution is void; and that courts, as well as other departments, are bound by that instrument.").

[252] Under well-established legal doctrine, consent exempts law enforcement officials from the need to obtain both a warrant and probable cause. Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

[253] *Id.* at 248–49.

[254] State v. Tate, 849 N.W.2d 798, 825–26 (Wis. 2014) (Abrahamson, C.J., dissenting).

[255] Riley v. California, 134 S. Ct. 2473, 2484 (2014).

[256] *See supra* note 43 and accompanying text.

[257] United States v. Davis, 754 F.3d 1205, 1216–17 (11th Cir. 2014) (adopting the Third Circuit reasoning to hold that "Davis has not voluntarily disclosed his cell site location information to the provider in such a fashion as to lose his reasonable expectation of privacy"), *reh'g en banc granted, opinion vacated*, 573 F. App'x 925 (11th Cir. 2014); *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317 (3d Cir. 2010) ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information. Therefore, [w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all." (internal citation omitted)).

[258] *See supra* Part III.D (discussing how the Third Party Doctrine is not relevant to ACSSs).

Despite a growing awareness of the depth of mass domestic surveillance conducted by the government, many Americans do not know the extent to which their cell phones provide detailed location and identity tracking.[259] Even those who know about the government's ability to obtain cell phone records from telecommunications carriers under ECPA cannot be expected to know about, much less voluntarily consent to, secret government surveillance.[260] Individuals thus enjoy a subjective expectation of privacy in the identifying and location information contained on their cell phones.

B. An Expectation of Privacy in One's Location and Identity Is Reasonable

After determining whether individuals display a subjective expectation of privacy, the Court must then decide whether society is prepared to recognize that expectation as "reasonable"[261] The Court measures this preparation in three principle ways: (i) the public frequently invades the subjective expectation of privacy, (ii) the surveillance intrudes upon a constitutionally protected space, and (iii) society ought to preserve the subjective expectation of privacy.

i. The Public Does Not Frequently or Routinely Obtain Identifying and Location Information from Others' Cell Phones

In the first instance, the Court sometimes determines whether an expectation of privacy is reasonable by whether the public frequently engages in behavior that allows it to obtain information similar to that gained by the surveillance. Under this approach, society cannot recognize an expectation of privacy in information that it regularly acquires through daily interaction. In *Bond v. United States*, for example, the government physically handled defendant's bag, stored in the overhead compartment of a Greyhound bus.[262] The Court held that despite the defendant having exposed the bag to members of the public, all of whom were capable of touching it, the officer's physical contact with the bag constituted a search because the defendant did not "expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner."[263] Likewise in *Kyllo*, the Court recognized government use of a thermal imaging device was a search because, *inter alia*, "the technology in question is not in general public use."[264]

The Court's aerial surveillance caselaw represents a slight variant on this approach, in which the public must have the technical and legal ability to routinely gather information similar to that obtained by law enforcement officials. In *California v. Ciraolo* and *Florida v. Riley*, the Court determined that defendants had no REOP in their homes and backyards vis-à-vis overflight because the plane and

[259] *Davis*, 754 F.3d at 1216–17; In re *Application*, 620 F.3d at 317; *Tate*, 849 N.W.2d at 825–26 (Abrahamson, C.J., dissenting) ("Although individuals may be generally aware that their locations may be tracked through their cell phones, most do not realize the extent of tracking possible and reasonably do not expect the cell phone service provider to report their precise location to law enforcement officers. It does not comport with the reality of the modern telecommunications age that individuals lose their constitutional right to privacy in their location simply by purchasing a cell phone.")
[260] Katz v. United States, 389 U.S. 347, 358 (1967) ("And, of course, the very nature of electronic surveillance precludes its use pursuant to the suspect's consent.").
[261] *Id.* at 361 (Harlan, J., concurring).
[262] Bond v. United States, 529 U.S. 334, 336 (2000).
[263] *Id.* at 338–39.
[264] Kyllo v. United States, 533 U.S. 27, 34 (2001).

helicopter used by law enforcement officers operated from a lawful public vantage point within publically navigable airspace.[265] In particular, the defendants' expectations of privacy were unreasonable because "'private and commercial flight . . . in the public airways is routine' in this country."[266] Justice O'Connor's crucial *Riley* concurrence[267] stressed the importance of frequency, noting that just because observation is legally possible does not mean that "an individual has no reasonable expectation of privacy from such observation."[268] Instead, the Court "must ask whether the helicopter was in the public airways at an altitude at which members of the public travel with sufficient *regularity*" to make reasonable Riley's expectation of privacy.[269]

Based on this standard, ACSS operations constitute a Fourth Amendment search. The public does not frequently operate devices that obtain the identity and location of all cell phone users in the immediate vicinity, nor do they have the legal and technical capabilities to routinely collect such data. Fourth Amendment protection will only last, however, for such time as individuals are able to preserve the secrecy of their identity and location from the general public. As digital technologies advance, the public may in fact be subjected to devices that obtain identifying and location information from surrounding individuals. Alternatively, devices and applications may stop giving users the ability to opt in to sharing their identities and locations with others. As the digital age expands, perfect secrecy from frequent public observation will no longer serve as an adequate proxy for privacy.

ii. ACSS Surveillance Intrudes Upon A Constitutionally Protected Space

In the second instance, the Court determines whether an expectation of privacy is reasonable by whether the surveillance intrudes upon a constitutionally protected space. In these spaces, the individual's expectation of privacy is presumed reasonable, as exemplified by the Court's consistent recognition that an individual's home is at the "very core of the Fourth Amendment."[270] In *Karo*, for example, the Court held unconstitutional the warrantless tracking of the ether container purchased by the suspected drug traffickers because the tracker "reveal[ed] a critical fact about the interior of the premises."[271]

Because ACSS operations, by definition, cannot identify the location of targets *ex ante*, law enforcement officials cannot assert that the surveillance will never implicate constitutionally protected

[265] Florida v. Riley, 488 U.S. 445, 451–52 (1989) (holding that the defendant did not have a REOP in his home and curtilage vis-à-vis observation from the air because the overflight was lawful); California v. Ciraolo, 476 U.S. 207, 213 (1986) (same).
[266] *Riley*, 488 U.S. at 450 (quoting *Ciraolo*, 476 U.S. at 215).
[267] A plurality of four justices wrote the opinion; Justice O'Connor concurred in judgment, and four justices dissented. Under the *Marks* rule of plurality interpretation, O'Connor's concurrence in *Riley* is arguably the narrowest possible ground agreed to by a majority of the Court. *See* Marks v. United States, 430 U.S. 188, 193 (1977). The plurality focused on whether the observation occurred from a lawful vantage point (encompassing vantage points both regularly and infrequently visited by the public), but Justice O'Connor focused on vantage points frequently visited by the public. *Riley*, 488 U.S. at 451–52, 453–54. Therefore, Justice O'Connor's requirement of "sufficient regularity" is the narrowest holding to which five Justices agreed.
[268] *Id.* at 453–54 (O'Connor, J., concurring in judgment).
[269] *Id.* (emphasis added).
[270] *See, e.g.*, *Kyllo*, 533 U.S. at 31 ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" (quoting Silverman v. United States, 365 U.S. 505, 511 (1961))).
[271] United States v. Karo, 468 U.S. 705, 715 (1984).

spaces such as the home. Indeed, of the known cases in which the government used an ACSS, all three resulted in law enforcement locating the phone in the constitutionally protected space of the home.[272] The possibility of invading this protected space classifies ACSS operation as a search, requiring a warrant. As held by the *Karo* Court, that law enforcement would have to obtain warrants in a large number of cases when using an ACSS "is hardly a compelling argument against the requirement."[273]

The Court's 2001 *Kyllo* decision represents a unique variation on the REOP presumption in constitutionally protected spaces. There, the Court held that when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[274] A stingray, likewise using electromagnetic radiation[275] to "see" into a home, aligns exactly with *Kyllo*: it is a device not in public use that allows a law enforcement officer to gain information about the interior of the home (i.e., that the identified cell phone, and thus its owner, is present) that she could not otherwise obtain without herself intruding into the home. As with the frequency approach, however, protecting intrusions caused only by technology not in general public use will survive only so long as ACSS technology remains outside common usage.[276]

iii. Society Should Recognize Affirmative Privacy Protections Divorced from Secrecy

The final approach shifts the privacy paradigm away from secrecy and towards affirmative protections.[277] Secrecy has never been a constitutional requirement; rather, courts adopted a secrecy-based measurement because in the pre-digital era, what we kept secret served as an effective proxy for what we considered private. As digital technology advances, however, the ability to keep information secret has shifted from an inevitable default to a chimera requiring substantial effort. In response, society must establish constitutional barriers around those activities and categories of information that it "is prepared" to recognize as private. A more affirmative notion of privacy aligns with the Constitution, which constructed a legal barrier to prevent the government from abusing its citizen-granted powers by violating citizen rights. As technology evaporates secrecy, the Court must establish new frameworks to preserve

[272] Thomas v. State, 127 So. 3d 658, 659–60 (Fla. Dist. Ct. App. 2013); United States v. Rigmaiden, No. CR 08–814–PHX–DGC, 2013 WL 1932800, at *3 (D. Ariz. May 8, 2013); State v. Tate, 849 N.W.2d 798, 803–04 (Wis. 2014). *See* United States v. Jones, 132 S. Ct. 945, 950 n.3 (2012) ("Where, as here, the Government obtains information by physically intruding on a constitutionally protected area, such a search has undoubtedly occurred.").
[273] *Karo*, 468 U.S. at 718 ("The argument that a warrant requirement would oblige the Government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement.").
[274] *Kyllo*, 533 U.S. at 40.
[275] Thermal or infrared radiation is another form of electromagnetic radiation. Police officers in *Kyllo* passively intercepted the infrared signals emanating outwards, making it more like a passive cell site simulator rather than an ACSS.
[276] Alternatively, the "general public use" requirement could be interpreted as a proxy to distinguish police conduct from public conduct (in line with the Fourth Amendment's prohibition of *government* intrusion). As a result, any law enforcement operation of stingrays would constitute a search, regardless of lay ACSS use. *See, e.g.*, State v. Davis, 321 P.3d 955, 962 (N.M. Ct. App. 2014), *cert. granted*, 324 P.3d 376 (N.M. 2014).
[277] *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.").

our rights to be free from unreasonable searches.

Examples of affirmative privacy protections have begun to appear in the Supreme Court's Fourth Amendment jurisprudence. In *Jones*, five Justices recognized that GPS monitoring of a person for 28 days constituted a search under the privacy paradigm—in spite of the inherent lack of secrecy in operating a car.[278] As Justice Alito observed in concurrence, "society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period."[279] Indeed, the entire foundation of the "mosaic theory" rests on the idea that "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance," regardless of whether the information obtained was kept secret.[280] And in *Riley*, the Court's most recent Fourth Amendment opinion, nine Justices so clearly recognized that law enforcement officers' access to the contents of a cell phone constituted a search—despite the access numerous third parties have to a cell phone user's emails, phone logs, photos, and locations—that they did not even consider the question.[281]

Forward-looking opinions from federal district and appellate courts have also begun to embrace affirmative privacy protections not grounded in secrecy. In *United States v. Vargas*, the Eastern District Court of Washington threw out six weeks of evidence obtained via a continuously recording video camera installed on a utility pole near the defendant's home.[282] Despite the legal ability of law enforcement officers to make "plain view" observations without a warrant,[283] and despite the camera's arguable similarity to a law enforcement officer standing near the defendant's home for six weeks, the court found the surveillance constituted an unreasonable search.[284] Americans, the court observed, have a reasonable expectation of privacy that "prohibits the warrantless, continuous, and covert recording of [their] front yard[s] for six weeks."[285]

In the 2014 case *United States v. Davis*, the Eleventh Circuit became the first federal appellate court to recognize a REOP in a single piece of cell site location information.[286] Although appearing to

---

[278] *Id.* at 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring in judgment).
[279] *Id.* at 964 (Alito, J., concurring in judgment).
[280] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd in part sub nom.*, United States v. Jones, 132 S. Ct. 945 (2012).
[281] Riley v. California, 134 S. Ct. 2473, 2492–93 (2014) (observing only once in passing that "[t]here is no dispute here that the officers engaged in a search of Wurie's cell phone").
[282] United States v. Vargas, No. CR-13-6025-EFS, slip op. at 2 (E.D. Wash. Dec. 15, 2014), *available at* http://cdn.arstechnica.net/wp-content/uploads/2014/12/sheaorder.pdf. The opinion is not currently published on Westlaw or Lexis.
[283] *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 213 (1986) ("The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible.").
[284] *Vargas*, No. CR-13-6025-EFS, slip op. at 21.
[285] *Id.*, slip op. at 2.
[286] United States v. Davis, 754 F.3d 1205, 1216 (11th Cir. 2014), *reh'g en banc granted, opinion vacated*, 573 F. App'x 925 (11th Cir. 2014). Two other federal circuit courts have found to the contrary. In 2010, the Third Circuit became the first circuit court to rule on the constitutional and statutory authority necessary to obtain historical location information from telecommunications carriers. *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 305–06 (3d Cir. 2010). The court refused to recognize a categorical REOP in location and movement information because the record demonstrated no evidence

operate within the frequent-public-access approach,[287] the Eleventh Circuit's circular reasoning resonates instead as affirmative protection of location information. The court held that an individual has a REOP in any "nonpublic" location information, which it defined as information shared with third parties but not "in a public way."[288] Because phones can accompany their users anywhere, "exposure of the cell site location information can convert what would otherwise be a private event into a public one."[289] Therefore, the court reasoned, location information is inherently "private in nature," protected even more than Jones' GPS data.[290]

The Sixth Circuit underwent similar legal analysis in extending Fourth Amendment protection to email content in *United States v. Warshak*. Law enforcement had exploited ECPA to obtain some 27,000 emails using an administrative subpoena.[291] After acknowledging Warshak's subjective expectation of privacy in his email,[292] the court upheld the reasonability of this expectation in spite of his Internet Service Provider's acknowledged ability, and even right, to access those emails.[293] The Fourth Amendment, the court held, "must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[294]

Just so with ACSS surveillance operations. Courts have a constitutional duty to prevent the government from engaging in unreasonable searches. Law enforcement agencies are already prohibited from warrantlessly touching bags to discern their contents,[295] bringing drug-sniffing dogs to front

---

that "historical CSLI, even when focused on cell phones that are equipped with GPS, extends to" the interior of the home. *Id.* at 312–13. The Third Circuit did, however, reject the applicability of the Third Party Doctrine, finding that "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information." *Id.* at 317–18. In 2013, the Fifth Circuit likewise denied constitutional protection for historical location information. *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 611–12, 614 (5th Cir. 2013). Contrary to its sister circuit, however, the court found that historical location information falls subject to the Third Party Doctrine because CSLI is a business record created by telecommunications carriers for legitimate business reasons, because subscribers are aware that they convey information to carriers, and because the use of a phone is voluntary. *Id.* This three-way circuit split indicates that the constitutional status of location information is in flux, with room for the courts to assert affirmative protections.

[287] *See supra* Part VI.B.i.

[288] *Davis*, 754 F.3d at 1216 ("In contrast, even on a person's first visit to a gynecologist, a psychiatrist, a bookie, or a priest, one may assume that the visit is private if it was not conducted in a public way.").

[289] *Id.*

[290] *Id.*

[291] United States v. Warshak, 631 F.3d 266, 282–83 (6th Cir. 2010). The SCA requires law enforcement officials to obtain a warrant to view electronic communications content held in storage by the Internet Service Provider ("ISP") for 180 days or less, but allows law enforcement to use an administrative subpoena to obtain the same emails if held in storage for more than 180 days. 18 U.S.C. § 2703 (2012). Here, law enforcement officer asked the ISP to archive all future messages emails (without his permission and contrary to usual practice), then obtained the emails with an administrative subpoena. *Warshak*, 631 F.3d at 283.

[292] *Id.* at 284.

[293] *Id.* at 286–88 ("As an initial matter, it must be observed that the mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy. . . . Consequently, we are convinced that some degree of routine access is hardly dispositive with respect to the privacy question.").

[294] *Id.* at 285.

[295] Bond v. United States, 529 U.S. 334, 339 (2000) ("We therefore hold that the agent's physical manipulation of petitioner's bag violated the Fourth Amendment.").

porches,[296] wiretapping conversations in public telephone booths,[297] intercepting thermal radiation emanating from the home,[298] placing GPS devices on cars,[299] searching cell phones,[300] and using electronic devices to determine "whether a particular article—or a person, for that matter—is in an individual's home at a particular time."[301] To bar these surveillance methods but condone the ability to secretly identify and track any citizen of this country flies in the face of the Fourth Amendment. ACSS operations, conducted without judicial oversight and without a showing of probable cause, violate an expectation of privacy that society can and should be prepared to recognize as reasonable.

VII. Interim Remedial Measures

The principal purpose of this Paper is to detail the legal arguments litigants can make when asserting that government use of an ACSS constitutes a Fourth Amendment search and consequentially requires a warrant supported by probable cause. Litigants can only argue for Fourth Amendment protections, however, if they know the government has used a stingray—something Part IV indicates would be fairly unlikely. Until the Supreme Court decisively addresses the constitutionality of ACSS operations, privacy advocates have several, albeit imperfect, alternative measures at their disposal.

Among the least-effective strategies, advocates can push agencies to engage in self-regulation by limiting their use of ACSSs and deleting all data obtained about non-targeted third parties. Self-regulation, however, is fundamentally flawed: the organizations charged with limiting their surveillance activities are also uniquely positioned to conduct secret ACSS operations without any independent oversight. Although the FBI has recently implemented regulations that mandate the acquisition of a search warrant prior to the use of an ACSS, agents have a number of exceptions, including in "cases that involve a fugitive" and when "the technology is used in public places or other locations at which the FBI deems there is no reasonable expectation of privacy"—exceptions so broad and subjective that they effectively swallow the self-imposed warrant requirement.[302]

Advocates can also urge judges to demand more detail and ask more questions when receiving law enforcement requests for court orders related to cell phone data.[303] For example, Superior Court

[296] Florida v. Jardines, 133 S. Ct. 1409, 1417–18 (2013) ("The government's use of trained police dogs to investigate the home and its immediate surroundings is a 'search' within the meaning of the Fourth Amendment.").
[297] Katz v. United States, 389 U.S. 347, 359 (1967) ("These considerations do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth. Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.").
[298] Kyllo v. United States, 533 U.S. 27, 40 (2001) ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").
[299] United States v. Jones, 132 S. Ct. 945, 949 (2012) ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.').
[300] Riley v. California, 134 S. Ct. 2473, 2495 (2014) ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").
[301] United States v. Karo, 468 U.S. 705,716 (1984) (We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual's home at a particular time.").
[302] Judiciary Committee Letter, *supra* note 177.
[303] *See* Fred Clasen-Kelly, *Judge Robert Bell: Secret Cellphone Tracking May Get More Scrutiny From*

judges in Pierce County, Washington, now require law enforcement officials to seek explicit permission when using an ACSS and swear by affidavit to not retain third party data.[304] So long as judges continue to issue orders for ACSS operations under the lower pen register/trap and trace standard, however, the benefits of this greater, albeit unstandardized, judicial scrutiny will be somewhat muted.

More practically, and now that ACSS operations have begun to receive greater media and legal scrutiny, defense attorneys should take a close look at any case involving evidence obtained through the use of a "pen register/trap and trace device." As outlined in Part IV, law enforcement officials frequently receive judicial authorization for the use of "pen registers" while failing to mention that an ACSS, rather than a telecommunications carrier, will be used to identify and track the defendant.[305] If discovery indicates that the government might have used a stingray, defense attorneys should file motions to suppress, challenging the operations as unconstitutional.[306] Only by challenging warrantless ACSS operations in court can the Judicial Branch finally consider their constitutionality.

At the state and local level, advocates can request that judges unseal court documents concerning pen register/trap and trace applications. They can also file open records requests. Although these applications have frequently been denied or blocked,[307] growing publicity and a requestor's ability to litigate have resulted in some recent successes.[308] These records and documents can provide concrete evidence about when, why, how often, and in what circumstances law enforcement agencies deploy ACSSs. Evidence of actual usage can be used to debunk law enforcement claims that ACSSs are used

---

Mecklenburg County Courts, CHARLOTTE OBSERVER (Nov. 29, 2014), http://www.charlotteobserver.com/2014/11/29/5351043/judge-robert-bell-secret-cellphone.html#storylink=cpy.

[304] Adam Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, TACOMA NEWS TRIBUNE (Nov. 15, 2014), http://www.thenewstribune.com/2014/11/15/3488642_tacoma-police-change-how-they.html?sp=/99/289/&rh=1 ("[Mecklenburg County] Superior Court Judge Robert Bell told the Observer he believes recent media coverage will prompt local judges to ask police when they plan to use a surveillance device, commonly called a StingRay, that law enforcement and the federal government have fought to shield from public view.").

[305] *See supra* note 173.

[306] *E.g.*, Mot. to Suppress Evidence at 2 & n.2, United States v. Harrison, Crim. No. CCB-14-170 (D. Md. Oct. 10, 2014), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/1371717/29-motion-to-suppress-stingray.pdf ("The Government has not specifically called the device a 'Stingray,' however the brief description of its use, as provided by the case agent and the prosecutor, is consistent with how a 'Stingray' is used."). *See also* Cyrus Farivar, *Murder-For-Hire Suspect Gets New ACLU Ally in Battle Against Phone Spying*, ARS TECHNICA (Nov. 26, 2014), http://arstechnica.com/tech-policy/2014/11/murder-for-hire-suspect-gets-new-aclu-ally-in-battle-against-phone-spying/ ("[Defense attorney] Brown told Ars that after having been a criminal defense attorney for a decade, he had never even heard of stingrays, much less dealt with them in a case. 'When it became apparent that it was used in my case, I started searching around and found some of the articles that [ACLU Attorney Nate Wessler] had posted, and I just called him to see what was out there,' he said.").

[307] *See supra* note 175 and accompanying text; Cyrus Farivar, ARS TECHNICA, *Dow Jones Asks Court To Unseal Long-Completed Digital Surveillance Cases*, (June 3, 2014), http://arstechnica.com/tech-policy/2014/06/dow-jones-asks-court-to-unseal-long-completed-digital-surveillance-cases/ (discussing how outgoing Magistrate Judge Brian Owsley decided "to unseal more than 100 of his own judicial orders involving digital surveillance that he himself had sealed at the government's request," only to see his order vacated by a U.S. district court judge, who ordered the records resealed and then sealed that order).

[308] *See* Cyrus Farivar, *Local Judge Unseals Hundreds of Highly Secret Cell Tracking Court Records*, ARS TECHNICA (Nov. 21, 2014), http://arstechnica.com/tech-policy/2014/11/local-judge-unseals-hundreds-of-highly-secret-cell-tracking-court-records/ (discussing the unsealing of "529 court documents in hundreds of criminal cases detailing the use of a stingray, or cell-site simulator, by local police"); Winkley, *supra* note 175.

rarely, only for emergencies, or only for serious criminal or terrorist threats.[309]

Finally, advocates can push for greater legal protections at the state level. Attorneys can challenge ACSS operations in state courts as violations of state constitutional law, which often extends beyond the Fourth Amendment. The Supreme Judicial Court of Massachusetts, for example, has held that law enforcement use of historical cell site location information (obtained from a telecommunications carrier) for location tracking constitutes a search under the Massachusetts Constitution., which suggests that the more invasive real-time tracking via stingray would also require a search warrant[310] The Supreme Court of New Jersey has similarly held that individuals retain REOP in their cell phone location data under the New Jersey Constitution and law enforcement officers can only obtain this data with a search warrant.[311] Advocates can also urge state legislatures to adopt proactive legislation that mandates search warrants for any law enforcement location tracking operation, as at least eleven states have done.[312] Since the vast majority of law enforcement operations take place under state law, these state-level statutory and constitutional protections offer the best hope for comprehensive judicial oversight of ACSS operations. Additionally, the ever-expanding number of state-based limitations on ACSS operations will give tangible proof for a nationwide sentiment that subjective expectations of privacy in one's cell phone are, in fact, reasonable.

VIII. Conclusion

An ACSS has the ability to identify and locate all cell phones—and therefore almost all persons—in the vicinity of the device. Law enforcement's ability to identify and track everyone, in secret

---

[309] *See* Adam Ashton, *'Stingray' Phone Trackers Facing More Scrutiny*, NEWS TRIBUNE (Nov. 15, 2014), http://www.thenewstribune.com/2014/11/15/3488645_stingray-phone-trackers-facing.html?sp=/99/296/&rh=1 (discussing how despite claims by the Tacoma Police Department to the local city council that they would use the ACSS to find bombs, the device has never been used to find explosive devices but instead has been used "to locate suspects wanted for crimes such as homicide, rape, robbery, kidnapping and narcotics trafficking"); *Lifting The Veil On Surveillance*, CHARLOTTE OBSERVER (Nov. 23, 2014), http://www.charlotteobserver.com/2014/11/22/5332855/lifting-the-veil-on-surveillance.html ("Also, despite CMPD and city officials indicating that the cell-site simulator technology would only be used in investigations involving serious felonies, some of the records show surveillance being used in lower-level cases.").

[310] Commonwealth v. Augustine, 4 N.E.3d 846, 850 (Mass. 2014).

[311] State v. Earls, 70 A.3d 630, 632 (N.J. 2013).

[312] S. B. 14-193, 69th Gen. Assemb., 2d Reg. Sess. (Colo. 2014), *available at* http://www.leg.state.co.us/clics/clics2014a/csl.nsf/billcontainers/1C1A65C619C7E9A187257C6F000271B1/$FILE/193_enr.pdf; Pub. Act 098-1104, 98th Gen. Assemb., Reg. Sess. (Ill. 2014), *available at* http://ilga.gov/legislation/publicacts/fulltext.asp?Name=098-1104; H. B. 1009, 118th Gen. Assemb., 2d Reg. Sess. (Ind. 2014), *available at* http://iga.in.gov/legislative/2014/bills/house/1009/#; Leg. Doc. 415, 126th Leg., 1st Reg. Sess. (Me. 2013), *available at* http://www.mainelegislature.org/legis/bills/bills_126th/chapters/PUBLIC409.asp; S. B. 0698, 2014 Gen. Assemb., Reg. Sess. (Md. 2014), *available at* http://mgaleg.maryland.gov/2014RS/bills/sb/sb0698E.pdf; S. B. SF 2466, 88th Leg., 3d Engrossment (Minn. 2014), *available at* https://www.revisor.mn.gov/bills/text.php?number=SF2466&version=3&session=ls88&session_year=2014&session_number=0; H. B. 603, 63rd Leg., Reg. Sess. (Mont. 2013), *available at* http://leg.mt.gov/bills/2013/billhtml/HB0603.htm; S. B. 2087, 108th Gen. Assemb., Reg. Sess. (Tenn. 2014), *available at* http://wapp.capitol.tn.gov/apps/Billinfo/default.aspx?BillNumber=SB2087&ga=108; H. B. 128, 2014 Leg., Gen. Sess. (Utah 2014), *available at* http://le.utah.gov/~2014/bills/static/hb0128.html; H. B. 17, 2014 Gen. Assemb., Reg. Sess. (Va. 2014), *available at* http://lis.virginia.gov/cgi-bin/legp604.exe?141+ful+HB17; Assemb. B. 536, 2013–14 Leg., Reg. Sess. (Wis. 2014), *available at* https://docs.legis.wisconsin.gov/2013/related/acts/375.

and without a warrant, is soberly reminiscent of the general warrants that the Fourth Amendment intended to prohibit.[313] Because ACSS operations both trespass upon an individual's property and violate an individual's reasonable expectation of privacy, they are Fourth Amendment searches. As a result, law enforcement agencies cannot use an ACSS without first obtaining a warrant based on probable cause.

Despite the pernicious capability of ACSSs, the scant information available about ACSS operations demonstrates that they are indeed a useful crime-fighting tool (e.g., by helping to locate a rape suspect[314]). Utility does not negate constitutional protections, but recognizing that an ACSS conducts a search requiring conformity with the Fourth Amendment does not bar law enforcement from using this technology. Warrants are not difficult to obtain,[315] and probable cause requires law enforcement officers to demonstrate only that "there is a fair probability that contraband or evidence of a crime will be found in a particular place."[316] What the Fourth Amendment does provide, however, is judicial oversight and accountability, ensuring that ACSS surveillance of cell phones does not exceed its probable cause scope or infringe on constitutional rights.

[313] *See* Payton v. New York, 445 U.S. 573, 583 (1980) ("It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment."); Boyd v. United States, 116 U.S. 616, 624–25 (1886) ("In order to ascertain the nature of the proceedings intended by the fourth amendment to the constitution under the terms 'unreasonable searches and seizures,' it is only necessary to recall the contemporary or then recent history of the controversies on the subject, both in this country and in England. The practice had obtained in the colonies of issuing writs of assistance to the revenue officers, empowering them, in their discretion, to search suspected places for smuggled goods, which James Otis pronounced 'the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book;' since they placed 'the liberty of every man in the hands of every petty officer.'").

[314] Thomas v. State, 127 So. 3d 658, 659–60 (Fla. Dist. Ct. App. 2013).

[315] Missouri v. McNeely, 133 S. Ct. 1552, 1561–63 (2013) (outlining how technology and procedural innovation has facilitated the speedy and efficient procurement of warrants).

[316] Illinois v. Gates, 462 U.S. 213, 238 (1983) ("The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.").